UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

DOCUMENTO ELETRÔNICO: ASPECTOS TÉCNICOS E REGULAMENTAÇÃO LEGAL

GILSON AMARAL DA SILVA
SANDRO MARCO FARIAS

ORIENTADOR:
ANDERSON C. A. NASCIMENTO

MONOGRAFIA DE ESPECIALIZAÇÃO

PUBLICAÇÃO: UNB.LABREDES.MFE.006/2006

BRASÍLIA/DF: AGOSTO/2006

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

DOCUMENTO ELETRÔNICO: ASPECTOS TÉCNICOS E REGULAMENTAÇÃO LEGAL

GILSON AMARAL DA SILVA
SANDRO MARCO FARIAS

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA.

APROVADA POR:

____

Anderson C. A. Nascimento, Doutor, UnB
(ORIENTADOR)

____

Georges Daniel Amvame-Nze, Mestre, UnB
(EXAMINADOR)

____

Odacyr Luiz Timm Júnior, Mestre, Tecsoft
(EXAMINADOR)

DATA: BRASÍLIA/DF, 28 DE AGOSTO DE 2006.

FICHA CATALOGRÁFICA

DA SILVA, GILSON AMARAL e **FARIAS, SANDRO MARCO**
Documento eletrônico: Aspectos técnicos e regulamentação legal [Distrito Federal] 2006
xii, p.186, 297 mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2006)
Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.
1. Criptografia 2. Legislação
3. Documento Eletrônico 4. Assinatura Digital
5. Certificação Digital 6. Validade Jurídica
I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

DA SILVA, G. A (2006), FARIAS, S. M. (2006) Documento eletrônico: Aspectos técnicos e regulamentação legal [Distrito Federal] 2006, Publicação UNB.LABREDES.MFE.006/2006, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 186 p.

CESSÃO DE DIREITOS

NOME DOS AUTORES: Gilson Amaral da Silva e Sandro Marco Farias
TÍTULO DA MONOGRAFIA: Documento eletrônico: Aspectos técnicos e regulamentação legal.
GRAU/ANO: Especialista/2006

____

Gilson Amaral da Silva

____

Sandro Marco Farias

AGRADECIMENTOS

Agradecemos...

Primeiramente a Deus por nos conceder saúde, força e discernimento, tornando possível a realização deste trabalho;

Ao nosso orientador, Prof. Dr. Anderson C. A. Nascimento pela presteza, incentivo e atenção no acompanhamento e orientação deste trabalho;

Ao Prof. Dr. Rafael Timóteo de Souza Jr. pelo apoio às nossas idéias iniciais e também pela coordenação do curso;

Aos nossos Professores que souberam nos guiar na busca de novos conhecimentos e horizontes, em especial ao Prof. Msc. Timm, pela organização deste curso;

Aos nossos colegas de trabalho e aos nossos chefes pela compreensão e apoio nos momentos em que estávamos cansados e não conseguimos dar o nosso melhor;

Aos colegas da biblioteca do Prodasen pela presteza e atenção no atendimento de nossas necessidades, inclusive obtendo livros em outras instituições;

A todos os nossos colegas pela convivência ao longo do curso, em especial a Patrícia Araujo da Cunha e Leopoldo Peres Torelly por não medirem esforços ao viabilizar o curso junto ao Senado Federal;

Ao PRODASEN, à Unilegis e à Unb pela viabilização e realização deste curso de Gestão em Tecnologia da Informação;

A todos os nossos amigos e familiares pelo suporte emocional e pelos momentos que foram subtraídos de nossa convivência ao longo do desenvolvimento deste trabalho;

Eu, Sandro, agradeço especialmente a minha mãe e a minha namorada pelo amor, compreensão e incentivo incondicionais nos momentos mais difíceis;

Eu, Gilson, agradeço a minha esposa, a minha filha de quase 2 anos e aos meus filhos adolescentes pelo carinho, compreensão e apoio durante todo o curso.

RESUMO

A sociedade da informação em que vivemos hoje é resultado do desenvolvimento das novas tecnologias de informação e comunicação, que por sua vez tem exigido das pessoas a necessidade onipresente de acesso rápido às informações e domínio da tecnologia. A utilização de documentos eletrônicos através da utilização de redes de comunicação, em especial a Internet, tem permitido a existência de acordos e contratos virtuais, ao mesmo tempo em que faz surgir novos desafios. A identificação da autoria e a preservação da integridade de um documento ou contrato eletrônico são os principais requisitos para a garantia da validade e eficácia jurídica dessas relações. A descoberta da criptografia assimétrica, utilizada em conjunto com uma infra-estrutura de certificação de chaves públicas (ICP), permitiu o desenvolvimento das técnicas que compõem a assinatura digital. A assinatura digital tem por objetivo assegurar a autenticidade e integridade de documentos ou mensagens eletrônicas, a fim de que os mesmos possam ser utilizados com segurança e forneçam maior eficácia probatória em caso de eventuais litígios. A legislação relacionada ao tema ainda não conseguiu acompanhar o mesmo ritmo da evolução tecnológica. Esse trabalho procura apresentar uma análise crítica das questões técnicas e legais relacionadas ao uso e à validade dos documentos eletrônicos, analisando também a legislação existente e as proposições em tramitação no Congresso Nacional.

ABSTRACT

The information society in which we live today is the result of the development of new communication and information technologies that have imposed on people the need to have quick access to information and working knowledge of the technology. The use of electronic documents via communication networks, especially the Internet, has allowed the emergence of virtual contracts and agreements while giving rise to a host of new challenges. The proper identification of a document’s authorship and its integrity are the main requirements to guarantee the validity, efficacy and legality of these agreements and contracts. The advent of asymmetric cryptography, used on top of a public key certification infrastructure (PKI), has fostered the development of the many techniques that make up a digital signature. The main goal of a digital signature is to attest the authenticity and integrity of electronic documents or messages in order to provide greater legal protection in case of litigation. Legislation related to this subject is struggling to keep up with the speed of the technology. This paper attempts to present a critical analysis of the many technical and legal issues related to the use and validity of electronic documents in light of the current legislation and law projects being considered by the Brazilian Congress.

ÍNDICE

ÍNDICE DE ABREVIAÇÕES

3DES	*Triple Data Encryption Standard*
AC	*Autoridade Certificadora*
AES	*Advanced Encryption Standard*
AR	*Autoridade de Registro*
BD	*Blu-Ray Disc*
CCJC	*Comissão de Constituição, Justiça e Cidadania*
CCTCI	*Comissão de Ciência e Tecnologia, Comunicação e Informática*
CD-R	*CD Recordable*
CD-ROM	*Compact Disc – Read Only Memory*
CEPESC	*Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações*
CESP	*Comissão Especial*
CF	*Constituição Federal*
CPI	*Comissão Parlamentar de Inquérito*
DES	*Data Encryption Standard*
DSA	*Digital Signature Algorithm*
DSS	*Digital Signature Standard*
DVD-ROM	*Digital Video Disc – Read Only Memory*
EC	*Emenda Constitucional*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
FIPS	*Federal Information Processing Standard*
GPL	*General Public License*
ICP	*Infra-estrutura de Chaves Públicas*
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
ITI	*Instituto Nacional de Tecnologia da Informacão*
LCR	*Lista de Certificados Revogados*

MIPS	*Milhões de Instruções por Segundo*
MP	*Medida Provisória*
MSC	*Mensagem no âmbito da Administração Pública Federal*
NIST	*National Institute of Standards and Technology*
OAB	*Ordem dos Advogados do Brasil*
PEC	*Proposta de Emenda à Constituição*
PEM	*Privacy Enhanced Mail Standard*
PIN	*Personal Information Number*
PKC	*Public Key Certificate*
PKI	*Public Key Infrastructure*
PL	*Projeto de Lei*
PLC	*Projeto de Lei da Câmara*
PLS	*Projeto de Lei do Senado*
RFC	*Request for Comments*
SHA	*Secure Hash Algorithm*
SPC	*Serviço de Proteção ao Crédito*
SPN	*Substitution-Permutation Network*
SSL	*Secure Sockets Layer*
TSA	*Time Stamping Authority*
UNCITRAL	*United Nations Commission on International Trade Law*
USB	*Universal Serial Bus*
WORM	*Write Once Read Many*

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

1. INTRODUÇÃO

Os documentos eletrônicos têm se tornado cada vez mais presentes no dia a dia das pessoas e organizações. O número de documentos elaborados ou disponíveis em meio eletrônico tem crescido de forma rápida e contínua. A necessidade prática de recuperação, manipulação e disseminação dessas informações tem mostrado que o gerenciamento de grandes volumes de informação em papel é dispendioso e, muitas vezes, ineficiente.

Com a popularização dos microcomputadores e o surgimento de redes de comunicação, em especial a Internet, o mundo nunca esteve tão perto de se tornar, de fato, a "aldeia global" a qual se referia Marshall Mcluhan[1], pesquisador canadense de comunicação em massa. Através da tecnologia hoje disponível, vemos surgir uma sociedade onde a informação é cada vez mais sinônimo de poder.

A utilização de navegadores com interface multimídia, associada ao uso de conexões de alta velocidade, têm estimulado o intercâmbio de dados sejam eles textos, imagens ou sons. Essa comodidade possibilitou o surgimento de novos serviços como a realização de transações eletrônicas e, em especial, aquelas relacionadas ao comércio eletrônico. O fato de serem eletrônicos não os torna essencialmente diferentes, uma vez que ambos representam uma manifestação de vontade das partes envolvidas, através de uma contratação eletrônica. A diferença está apenas no suporte, ou seja, na substituição do papel pela mídia eletrônica.

Entretanto, o uso da tecnologia digital, ao agregar comodidade e rapidez nos processos, traz também um aumento no número de fraudes. Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), mantido pelo Comitê Gestor da Internet (CGI), o número de tentativas de fraudes bancárias e financeiras no período compreendido entre 1999 e 2005 cresceu de forma exponencial [1].

Esse crescimento está diretamente relacionado as características intrínsecas dos documentos eletrônicos e às falhas de identificação dos usuários e sistemas envolvidos. Isso tem representado um grande desafio técnico e jurídico, em razão da rápida evolução tecnológica e da dificuldade de adaptação ou criação de novos instrumentos jurídicos.

Essa nova realidade é destacada no "Livro Verde para a Sociedade da Informação em Portugal", elaborado pelo Ministério da Ciência e Tecnologia em Lisboa:

---

[1] Marshall McLuhan foi um visionário educador da mídia em massa. "*The medium is the message*", talvez a sua frase mais famosa, era uma de suas avançadas percepções do impacto da mídia na sociedade.

> “*A sociedade da informação, pela sua própria natureza e novidade intrínseca, levanta na sua implementação um conjunto de questões de índole legislativa e administrativa. Neste sentido, novos domínios da Sociedade da Informação carecem de regulação adequada contemplando a proteção de valores básicos comuns à civilização do Estado de Direito e da democracia.*” [2]

O surgimento das assinaturas digitais em conjunto com a certificação digital permitiu um avanço tecnológico que tem sido amparado juridicamente pela Medida Provisória 2.200-2 de 24 de agosto de 2001, que instituiu a Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil). Entretanto, em razão da interdisciplinaridade e complexidade do assunto, muitas questões podem ser discutidas com a sociedade de forma a tornar mais transparente essa importante mudança de paradigma: a utilização de documentos e contratos eletrônicos com validade e eficácia jurídica.

Esse trabalho procura apresentar uma análise crítica das questões técnicas e legais relacionadas ao uso e à validade dos documentos eletrônicos, analisando também a legislação existente e as proposições em tramitação no Congresso Nacional.

Os capítulos 1 e 2 apresentam respectivamente uma introdução ao assunto e os objetivos a serem alcançados por essa monografia. O capítulo 3 estabelece um paralelo entre os documentos tradicionais e os documentos eletrônicos, suas características e particularidades, bem como os requisitos para obtenção de eficácia e validade jurídica.

Os capítulos 4, 5 e 6 apresentam o embasamento necessário para o entendimento das questões técnicas relacionadas a assinatura digital, que é um dos elementos que propiciam à obtenção da autenticidade e da integridade de um documento eletrônico. O capítulo 4 apresenta os conceitos básicos da criptografia, incluindo a criptografia de chaves públicas ou assimétrica, base para o desenvolvimento das técnicas que possibilitaram o surgimento da assinatura digital. O capítulo 5 traz uma introdução às assinaturas digitais e apresenta os principais algoritmos de assinatura, incluindo as funções de resumo de uma mensagem (“*hash*”). O capítulo 6 apresenta a importância da existência de uma infra-estrutura de chaves públicas (ICP), trata dos vários aspectos relacionados aos certificados digitais e apresenta a infra-estrutura de chaves brasileira ICP-Brasil.

A partir dessas informações, o capítulo 7 trata da regulamentação legal dos documentos eletrônicos e das assinaturas digitais. Inicialmente, são citadas as principais leis existentes no mundo e depois é apresentada a legislação brasileira começando com uma breve introdução ao processo legislativo e seus elementos. O capítulo 8 apresenta uma análise

crítica em relação aos documentos eletrônicos e à assinatura digital. O mesmo analisa diversas questões técnicas e legais, apresentando inúmeras considerações e um exemplo prático, que mostra como poderia ser um fluxo de contratação eletrônica. Constitui o capítulo de maior relevância para este trabalho.

Por fim, o capítulo 10 apresenta as conclusões desse trabalho, baseadas nas análises realizadas no capítulo 8 e também considerando a utilização prática de documentos eletrônicos que contém assinaturas digitais. O capítulo 11 apresenta os anexos I e II tratando respectivamente do conteúdo da legislação brasileira existente (íntegra de projetos de lei, decretos e medidas provisórias citados nesse trabalho) e de uma comparação sucinta entre as diversas leis existentes em outros países.

2. OBJETIVO

O objetivo deste trabalho é apresentar uma análise crítica sobre as questões técnicas e legais relacionadas ao uso e à validade de um documento eletrônico digital. Para isso, é estabelecido um paralelo entre os documentos tradicionais e eletrônicos e são fornecidos subsídios ao entendimento dos requisitos essenciais de autenticidade, integridade e tempestividade. Esses requisitos permitem que um documento eletrônico digital possa alcançar validade e eficácia jurídica. A forma de obtenção desses requisitos surgiu de inovações tecnológicas que apresentam desafios para a adequação e elaboração de novas leis. Essas questões técnicas e a necessidade de amparo legal constituem objeto principal de análise deste trabalho.

Há também um caráter educativo nesta monografia, na medida em que a mesma pode ser utilizada como material de referência em relação aos temas documento eletrônico, assinatura digital e legislação relacionada.

3. DOCUMENTO TRADICIONAL VERSUS DOCUMENTO ELETRÔNICO

3.1. CONTEXTO HISTÓRICO

O ser humano sempre tentou deixar traços de sua existência e de sua cultura para as futuras gerações. Quando o homem da caverna rabiscava na pedra cenas de caçadas e lutas, enfim retratos do seu cotidiano, sequer tinha noção de que estava exercendo uma atividade de documentação.

Com o advento da escrita cuneiforme pelos sumérios a mais de 3.500 anos AC, o conhecimento passou a ser entendido de uma maneira mais uniforme, diminuindo drasticamente o grau de subjetividade antes existente. Dessa forma, a informação original estava apta a se perpetuar ao longo do tempo.

O termo documento tem origem no latim *documentum*, que por sua vez deriva do verbo *docere* que em latim significa ensinar, indicar [3]. Essa origem revela uma característica essencial de um documento – sua finalidade de transmitir informações.

Com a utilização de suportes materiais resistentes (pedra, cerâmica, papiro, pergaminho e finalmente o papel) é que o documento foi associado a algo tangível, palpável. Esse fato, associado à portabilidade e a possibilidade de disseminação da informação, é que mais tarde permitiu o surgimento dos códigos de leis, do livro, da literatura e tantas outras formas da expressão do conhecimento.

Segundo o dicionário "Novo Dicionário Aurélio da Língua Portuguesa"[4], a palavra documento significa:

1. *Qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc.*
2. *Escritura destinada a comprovar um fato; declaração escrita, revestida de forma padronizada, sobre fato(s) ou acontecimento(s) de natureza jurídica.*
3. *Qualquer registro gráfico.*
4. *Qualquer arquivo com dados gerados por um aplicativo, geralmente aquele criado em processador de textos.*

Como foi citado anteriormente, o conceito de documento não tem uma relação necessária com o papel, significando apenas a fixação do conhecimento ou da informação, para acesso e posterior comprovação, independentemente do meio utilizado. Na verdade não

existe diferença semântica entre o documento tradicional e o documento eletrônico – ambos representam um fato. A diferença está apenas no suporte, na substituição do papel pela mídia eletrônica, seja ela um disquete, um CD ou até mesmo um arquivo no disco rígido do computador.

Atualmente, após o advento da informática e também da rede Internet, o volume de informações disponíveis à sociedade tem crescido exponencialmente. Embora as informações armazenadas em computadores ainda sejam poucas em relação ao total, a tendência é que cada vez mais o papel perca espaço para a mídia eletrônica. Isso não se deve somente as dificuldades de manuseio e tratamento da informação, mas também ao alto custo relacionado a essas atividades.

Como é possível perceber, o reinado do documento tradicional escrito em papel, embora ainda distante de terminar, com certeza já teve o seu apogeu.

3.2. DOCUMENTO TRADICIONAL

Os itens a seguir buscam esclarecer os diversos conceitos utilizados e características dos documentos tradicionais. A correta interpretação dos mesmos é muito importante para a compreensão deste trabalho.

Suporte material

Entende-se por suporte material ou suporte físico, a própria matéria da qual é formado fisicamente o documento. O suporte, segundo ZAGAMI [5], "é uma substância que permite a fixação dos signos gráficos no qual é expresso o documento. O mais comum dos suportes à escrituração é a carta, mas os mais variados tipos de suporte são abstratamente concebíveis". Atualmente, o suporte mais utilizado em documentos é o papel, que acredita-se tenha sido inventado na China no ano de 105 DC [6]. Outros exemplos de suporte material são a cerâmica, a pedra, o pergaminho, o papiro, a cera, o metal, que também têm a capacidade de registrar um fato.

Meio

O meio é a forma utilizada para representar uma informação, um fato. O meio pode ser uma gravura, um símbolo, um mapa, um desenho. Entretanto, o meio mais tradicional utilizado para representar um documento é o uso da escrita. O uso da escrita (meio) em papel (suporte) permitiu o registro preciso e durável de informações. A aceitação,

popularidade e adequação do método para o registro de uma informação foi tão grande, que isso explica a imensa quantidade de documentos que assim foram produzidos e continuam a ser até os dias de hoje.

Indissociabilidade entre o suporte físico e seu conteúdo

O conteúdo é qualquer fato, expressão do pensamento, ou manifestação de vontade que possa ser representado utilizando-se um suporte físico e um meio apropriado. Um documento tradicional em papel tem como característica primária a indissociabilidade entre o conteúdo e o seu suporte físico. Ou seja, não é possível passar o conteúdo de um documento para outro suporte físico sem que essa ação não resulte na destruição do documento original. Assim, qualquer reprodução do conteúdo terá que obrigatoriamente ser feita em outro suporte físico, através de uma imitação, o que não garantirá as suas características originais, dado que o suporte da cópia nunca será idêntico ao do original.

Autoria

O elemento mais comum para atestar a autoria de um documento é através da identificação de sua assinatura. Segundo SANTOS [7], “Autor do documento é a pessoa a quem se atribui a sua formação, isto é, a quem se atribui a sua paternidade”. O artigo 371, do Código de Processo Civil, diz: “Reputa-se autor do documento particular: I – aquele que o fez e o assinou; II – aquele, por conta de quem foi feito, estando assinado; III – aquele que, mandando compô-lo, não o firmou, porque, conforme a experiência comum, não se costuma assinar, como livros comerciais e assentos domésticos”. Quanto aos documentos públicos, reputa-se seu autor o oficial público que os lavrou, embora todos os que os subscrevam também possam ser assim considerados [8].

Via de regra, salvo os documentos em que “não se costuma assinar”, a autoria do documento é provada pela assinatura do autor.

Data de criação

Segundo o art. 370 do Código de Processo Civil, “a data do documento particular quando a seu respeito surgir dúvida ou impugnação entre os litigantes, provar-se-á por todos os meios de direito. Mas, em relação a terceiros, considerar-se-á datado o documento particular: I – no dia em que foi registrado; II – desde a morte de algum dos signatários; III – a partir da impossibilidade física, que sobreveio a qualquer dos signatários; IV – da sua apresentação em repartição pública ou em juízo; V – do ato ou fato que estabeleça, de modo

certo, a anterioridade da formação do documento". Em relação aos documentos públicos, dada a fé pública de quem os lavrou, a data do documento público é presumida verdadeira.

Assinatura

A assinatura é a forma mais comum de comprovação da autoria de um documento. Ela é única e exclusiva porque corresponde à escrita manual do signatário, podendo ainda ser submetida à perícia através de exame grafológico.

3.3. REQUISITOS PARA EFICÁCIA DA PROVA DOCUMENTAL

Um documento pode ser considerado um elemento de prova desde que atenda aos seguintes requisitos básicos: autenticidade[2], integridade[3] e tempestividade[4]. Esses requisitos normalmente estão relacionados ao suporte físico a que pertence o documento e, desde que sejam adequadamente preenchidos, fornecem elementos suficientes para garantir eficácia jurídica probatória. Esses elementos são descritos com mais detalhes a seguir.

Autenticidade

Por autenticidade entende-se a certeza de que o documento provém do autor nele indicado. É autêntico o documento quando verdadeiramente elaborado pelo autor nele declarado [7]. Em documentos escritos, na grande maioria das vezes, o que comprova a autoria é a aplicação da assinatura no mesmo papel onde se encontram o restante das informações.

Integridade

A integridade é característica daquilo que se apresenta ileso, intacto, íntegro. Um documento é considerado íntegro quando não houve adulteração do seu conteúdo posterior a sua criação. Segundo TRUJILLO [9], "o valor probatório do documento – seja em que base material esteja "inscrito" – está na dependência de que esse suporte material deva ser indelével, ou seja, que não permita qualquer tipo de adulteração, deliqüescência ou cancelamento que de outra forma não possa ser percebido".

---

[2] Código de Processo Civil, arts. 369, 371, 373, 374
[3] Código de Processo Civil, arts. 365, 375, 383-386
[4] Código de Processo Civil, art. 370

Tempestividade

A palavra tempestividade é muito usada nos meios jurídicos para designar "dentro do prazo" e segundo o Dicionário Houaiss da Língua Portuguesa [10] quer dizer "qualidade ou característica daquilo que ocorre no momento certo, oportuno". Assim, a tempestividade de um documento serve para comprovar que a data do fato representado é compatível com a idade do papel utilizado como suporte. Esse cuidado visa garantir que um documento não tenha sido produzido para comprovação de um fato anterior a ele, conforme cita THEODORO JÚNIOR [11]: "pode surgir controvérsia não sobre o teor das declarações de vontade contidas em um documento, mas apenas quanto à época em que foram manifestadas".

3.4. DOCUMENTO ELETRÔNICO

Pode-se definir um documento eletrônico como sendo uma seqüência de bits, que traduzida por meio de um determinado programa de computador, é representativa de um fato [12]. O termo eletrônico, segundo o "Novo Dicionário Aurélio da Língua Portuguesa" [4], é um adjetivo que diz respeito à "*parte da física dedicada ao estudo do comportamento de circuitos elétricos que contenham válvulas, semicondutores, transdutores, etc., ou à fabricação de tais circuitos*". Portanto, os documentos eletrônicos, não são em sua essência eletrônicos, porém dependem de máquinas eletrônicas para serem visualizados.

Considerando os documentos que são criados e representados com o auxílio de um computador, seria mais apropriado denominá-los de documentos digitais, pois em última análise são compostos de dígitos binários (bits). Porém, a fim de seguir a palavra de uso mais comum, nesse trabalho será utilizado o termo "documento eletrônico" para identificar as informações manipuladas, armazenadas e representadas com o uso de um computador.

É importante salientar que segundo GIANNANTONIO [13], "distinguem-se documentos eletrônicos *stricto sensu* (senso estrito), memorizados em forma digital e não perceptíveis ao homem senão através do computador, e documentos eletrônicos *lato sensu* (senso amplo), isto é, todos os documentos formados pelo computador mediante dispositivos de saída". Observe-se que nesse segundo tipo, os documentos não existem em forma exclusivamente digital, como é o caso, de um documento produzido por uma impressora – apenas foram criados através do uso do computador. No contexto desse trabalho serão considerados os documentos eletrônicos de senso estrito, ou seja, aqueles que se encontram

em forma digital, compostos por bits e perceptíveis somente através do uso de computador em conjunto com a utilização de um programa adequado (*software*).

Segundo MARCACINI [14], "da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser um desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital".

Deve-se levar em conta também que um documento tradicional pode ter um ou mais originais e várias "cópias". No meio eletrônico, esse conceito não se aplica, pois dado que a seqüência de bits que formam o documento pode ser reproduzida infinitas vezes, mantendo-se exatamente igual a matriz, não é possível referir-se ao original, a cópia ou número de vias de um documento eletrônico. Diante dessa situação, a abordagem relacionada ao entendimento da eficácia probatória dos documentos eletrônicos tem que ser um pouco diversa daquela utilizada nos documentos tradicionais. Para que se possa entender melhor essa questão, vários conceitos relacionados aos documentos eletrônicos, inclusive a utilização de certificados digitais, serão discutidos nos itens a seguir.

3.5. PROPRIEDADES DOS DOCUMENTOS ELETRÔNICOS

O documento tradicionalmente considerado não mais se adapta à necessidade moderna de propiciar uma maior agilidade em relação à circulação da informação. É mister esclarecer e confrontar as características dos documentos eletrônicos que os tornam mais adequados para utilização na "sociedade da informação" em que vivemos hoje.

O entendimento dessas questões permitirá entender que, embora os requisitos para obtenção de eficácia probatória dos documentos eletrônicos sejam os mesmos dos documentos tradicionais (autenticidade, integridade e tempestividade), a forma de obtê-los e comprová-los é diferente.

Facilidade de disseminação e dissociabilidade

Como os documentos eletrônicos não estão presos a um suporte físico ao qual estão armazenados, os mesmos podem ser transmitidos de um local para outro com extrema facilidade. Pelo fato de estarem na forma digital, essa cópia é, em todos os sentidos, idêntica ao original. Independentemente de onde o arquivo venha a ser armazenado e de quantas transferências sucessivas tenham sido feitas, pode-se dizer que todos os documentos

transmitidos são perfeitamente idênticos. Por fim, os dados que compõem um documento eletrônico são facilmente dissociáveis de seu suporte que é a mídia eletrônica.

Alterabilidade

Os documentos eletrônicos, uma vez que em última análise podem ser considerados arquivos de um computador ou de qualquer outra mídia de armazenamento, podem ser alterados sem qualquer restrição. Essa é uma característica de sua própria existência e que garante sua grande flexibilidade.

Deve-se ressaltar que não está sendo levada em consideração a utilização de mídias que não permitem a regravação dos dados após a sua gravação (CD-ROM, por exemplo), nem de mecanismos de proteção como a utilização de senhas. Além do conteúdo do documento, é possível alterar atributos do arquivo, como por exemplo**,** a data e hora de sua criação/alteração. Mais importante ainda é perceber que a alteração de um documento pode não deixar vestígios, de modo que não há maneira de identificar o original daquele que foi alterado.

Facilidade de processamento

A facilidade de processamento refere-se a capacidade inerente aos documentos eletrônicos de poderem ser facilmente manipuláveis, ou seja, existem inúmeras possibilidades de utilização dos dados, como consultas, cruzamento de dados, comparações, todas realizadas eletronicamente através da utilização de programas apropriados.

Economia de espaço e facilidade de preservação

É inegável que as informações armazenadas de forma eletrônica ocupam infinitamente menos espaço do que aquelas armazenadas através de documentos tradicionais em papel. A título de exemplificação, calcula-se que um processo com trinta e oito volumes, correspondente a 11.500 folhas de papel, pode ser convertido em um único CD-ROM [15]. Além desse fato, temos o DVD que pode armazenar aproximadamente 6,5 vezes o conteúdo de um CD-ROM, não mencionando a popularização eminente de novas mídias como o Blu-Ray (BD) com capacidade de 25 Gb (face simples) ou 50 Gb (face dupla) o que equivaleria a aproximadamente a capacidade de 79 CD-ROMs. Por fim, tomando-se as precauções necessárias, como verificação periódica do estado da mídia e cópias de segurança, a conservação de uma mídia eletrônica é mais fácil, barata e prática do que a conservação de volumes de papel.

3.6. VALIDADE DOS DOCUMENTOS ELETRÔNICOS

Diante das características anteriormente apresentadas, neste tópico serão abordados os requisitos para obtenção da validade jurídica dos documentos eletrônicos, as tentativas iniciais de obter a equivalência do documento eletrônico com o documento tradicional e a solução tecnológica aceita hoje em dia com a utilização das assinaturas digitais, baseadas na técnica de criptografia assimétrica. Essa técnica, em conjunto com a emissão de certificados digitais, permite a aposição e a verificação eletrônica da assinatura em um documento digital.

3.6.1. Requisitos para obtenção da validade jurídica dos documentos eletrônicos

Apesar das peculiaridades de um documento eletrônico, percebe-se que o mesmo apenas terá validade jurídica se atender às mesmas exigências demandadas do documento físico, ou seja, se for possível a verificação da autoria, da integridade e da data de sua criação.

Diante das peculiaridades de um documento eletrônico, segundo SANTOLIM [16], o documento eletrônico deve possuir as seguintes características:

1. Permitir livremente a inserção dos dados ou da descrição dos fatos que se quer registrar;
2. Permitir a identificação das partes intervenientes, de modo inequívoco, a partir de sinal ou sinais particulares;
3. Não poder ser alterado sem deixar vestígios localizáveis, ao menos através de procedimentos técnicos sofisticados, assim como ocorre com o suporte tradicional em papel.

A dissociabilidade de um documento eletrônico em relação ao seu suporte, tem como conseqüência principal a facilidade de alteração do seu conteúdo. Como não há distinção entre original e cópia, a alteração de um documento digital pode ser difícil, ou até mesmo impossível de ser detectada. Assim, os elementos de validação devem estar vinculados ao conteúdo, e não ao suporte, como ocorre no documento físico, considerando que neste último há a inseparabilidade entre conteúdo e suporte, o que não ocorre no primeiro.

Com o impacto trazido, por exemplo, pelo comércio eletrônico na sociedade atual, é indispensável o adequado reconhecimento legal dos acordos e contratos efetuados eletronicamente, de maneira que seja possível utilizar os documentos eletrônicos digitais como meio de prova, perfeitamente válido, em eventual litígio judicial [17].

3.6.2. Tentativas de obtenção de um documento eletrônico imputável

Uma vez descritos os requisitos essenciais para a obtenção de validade jurídica dos documentos eletrônicos, é importante tomar conhecimento de algumas idéias iniciais que procuraram atingir esse objetivo, mesmo aquelas que não obtiveram pleno êxito.

Inicialmente pensou-se na utilização de mídias eletrônicas não regraváveis (do tipo WORM – *Write Once Read Many*), como suporte físico aos documentos eletrônicos de maneira que os mesmos se tornassem indeléveis, que não pudessem ser alterados ou apagados (o tipo mais comum desse tipo de mídia é o CD-R ou CD gravável). Esse tipo de mídia não permite a alteração dos dados uma vez gravados e isso seria uma forma de garantir a integridade do conteúdo gravado. Entretanto, não há uma forma prática de comprovar a autenticidade dos documentos gravados e a própria evolução da tecnologia encarregou-se de encerrar a idéia. Hoje um CD-R permite a gravação de dados em sessões (ISO/IEC 13490), onde apenas uma sessão pode estar ativa por vez, o que possibilitaria a substituição ou modificação de dados após a gravação inicial, através da criação e ativação de uma nova sessão.

Para resolver a questão da autenticidade, surgiu a idéia da assinatura digitalizada. A assinatura digitalizada é obtida com a utilização de um "*scanner*" que cria uma imagem da assinatura (digitalização), posteriormente salva em um arquivo apropriado. Esse processo é análogo a uma cópia reprográfica que pode ser reproduzida infinitas vezes, com o agravante de que a assinatura digitalizada pode ser facilmente copiada e afixada em qualquer documento. Conclui-se que a assinatura digitalizada não tem caráter probatório, não sendo possível a sua equiparação com a assinatura tradicional aposta em papel. Entretanto, é oportuno mencionar esse tipo de assinatura em contraste com as assinaturas eletrônicas, em especial a assinatura digital, de nome parecido mas utilização e possibilidades totalmente distintas.

A utilização de senhas ou PIN (*Personal Identification Number*) – um conjunto de quatro ou mais dígitos – muito comum nos caixas eletrônicos e no comércio eletrônico via Internet, também não fornece todos os elementos necessários para a criação de um documento eletrônico imputável. Embora a senha ou PIN sejam pessoais, nem sempre são de conhecimento exclusivo do usuário, uma vez que têm que ser conferidos através de um sistema qualquer de verificação ou até mesmo podem ser obtidos por meios fraudulentos. A contraparte de uma negociação, um banco por exemplo, possui todas as informações

necessárias para gerar um registro que simule qualquer operação, exatamente como seria feito caso tivesse sido realizada por um usuário, através do uso de sua senha pessoal.

O uso da identificação biométrica, que baseia-se nas características físicas e comportamentais do ser humano, foi também uma possibilidade estudada. Essas características permitem que uma determinada pessoa seja identificada unicamente, através da utilização de traços pessoais únicos de cada pessoa (a impressão digital, o desenho da íris, o timbre da voz, entre outros) [18]. A firma biométrica seria exclusiva e reconhecível, podendo ser imputável a uma e somente uma determinada pessoa. O que se verifica na prática é a dificuldade de integração de uma firma biométrica com os requisitos essenciais de uma assinatura. A firma biométrica pode suprir o requisito da identificação da autoria e em conjunto com um suporte indelével poderia também fornecer o requisito da integridade. Porém, uma vez aposta em um documento eletrônico, nada impediria a sua reusabilidade uma vez que não apresenta nenhum vínculo direto com o conteúdo de um documento. Na prática, a identificação biométrica fornece um método de autenticação importante, mas deve ser usada em conjunto com outras técnicas que veremos adiante, para garantir o requisito de integridade de um documento eletrônico.

3.6.3. A utilização de criptografia e certificados digitais

A descoberta da criptografia de chaves públicas [19] e posterior criação do algoritmo para assinatura digital denominado RSA [20], permitiu uma forma de garantir a autenticidade e integridade de um documento eletrônico. Um algoritmo de assinatura digital permite que uma pequena quantidade de dados sejam criados e anexados ao documento original utilizando-se uma chave secreta (senha). Através de uma outra chave, denominada de chave pública, é possível verificar se a assinatura realmente foi gerada com o uso da chave privada correspondente. Como a assinatura está intrinsecamente relacionada ao documento assinado, qualquer alteração no mesmo será indicada pela invalidação da assinatura garantindo o requisito de integridade.

Como as chaves pública e privada são geradas aos pares e estão matematicamente relacionadas, a verificação de uma assinatura feita com a chave privada é realizada através de sua correspondente chave pública, garantindo-se o requisito de autenticidade (autoria), uma vez que somente o detentor da chave privada poderia ter assinado o documento em questão. Para garantir que uma determinada chave pública pertença realmente a uma determinada pessoa, foram criados os certificados digitais. Um certificado digital nada mais é do que um

arquivo que contém um vínculo entre uma chave pública e a identificação de uma pessoa ou entidade garantidos (assinados) por uma autoridade competente (denominada de Autoridade Certificadora – AC). O uso das assinaturas digitais, dos certificados digitais e de uma infra-estrutura apropriada de chaves públicas, possibilita um método de garantir tecnicamente os pré-requisitos para que um documento possa ser juridicamente considerado.

Os próximos capítulos apresentam uma introdução a criptografia e um detalhamento maior a respeito das assinaturas digitais, explorando conceitos necessários para que se possa analisar as questões técnicas e legais relacionadas a validade de um documento eletrônico.

4. CRIPTOGRAFIA

4.1. INTRODUÇÃO

Para avançar na análise da validade jurídica do documento digital, torna-se necessária uma introdução aos conceitos básicos de criptografia, cujas técnicas são primordiais para fornecer ao documento digital os elementos capazes de lhe atribuir validade jurídica.

A palavra criptografia vem do francês "*cryptographie*" que é oriunda da junção das palavras gregas "*kriptós*" (escondido, oculto, secreto) e "*gráphein*" (escrever, descrever) [21]. Assim, a criptografia pode ser definida como a ciência e arte de transformar uma mensagem escrita, clara, em outra também escrita e legível, cifrada, inteligível para outrem que não o destinatário, conhecedor da convenção empregada na cifragem [22].

Na criptografia, o texto inicial, legível para todos, é denominado texto em claro (do inglês "*plaintext*"). O processo de codificação de um texto em claro é denominado cifragem, e o texto codificado recebe o nome de texto cifrado (do inglês "*cyphertext*"). A recuperação do texto inicial recebe o nome de decifragem. Com a utilização dos computadores, o que é cifrado são arquivos que contém dados digitais (bits), de forma que não somente textos, mas arquivos contendo qualquer tipo de informação (fotos, sons, vídeos, planilhas, etc) podem ser cifrados utilizando a mesma técnica. Também são muito utilizados os termos "criptografar" e "descriptografar" ou "decriptar" como sinônimo de cifrar e decifrar respectivamente. Entretanto, cabe observar, que embora o termo "criptografar" exista em qualquer dicionário da língua portuguesa, o seu correspondente "descriptografar" é um verbete inexistente. Interessante observar também que o termo "decriptar" existe no dicionário Aurélio [4] como antônimo de "criptografar" e não existe no novo dicionário Houaiss [10].

A utilização da criptografia existe desde a Antiguidade e, segundo KAHN [23], uma inscrição de hieroglifos fora do padrão datada de 1.900 A.C. é tida como o primeiro exemplo escrito de seu uso. Nessa época, as cifras hebraicas foram as que ficaram mais conhecidas (600 – 500 A.C.). Essas cifras eram realizadas através de uma substituição monoalfabética e assim esses métodos criptográficos eram baseados no segredo dos algoritmos utilizados. Um simples estudo estatístico da língua utilizada era suficiente para decifrar o texto original [24]. Somente com o surgimento do computador eletrônico, logo

após a 2ª Guerra Mundial, que a pesquisa em criptografia evoluiu qualitativamente e passou-se a utilizar complexos cálculos matemáticos. Hoje, os algoritmos modernos são todos publicamente conhecidos e baseiam-se no segredo da chave e não do próprio algoritmo.

Existem duas formas de utilização de criptografia com o uso de chaves: a criptografia convencional ou simétrica e a criptografia assimétrica ou de chaves públicas. O primeiro utiliza uma única chave para cifrar e decifrar a mensagem. Assim, para garantir o sigilo da informação, apenas o emissor e o receptor devem conhecer a chave. O problema desse modelo reside exatamente nessa questão: a chave utilizada para cifrar a mensagem deve ser compartilhada com todos os que precisam ler a mensagem, o que cria dificuldades na distribuição da chave e na manutenção de seu sigilo.

Já a criptografia assimétrica, de especial relevância para o correto entendimento do funcionamento da assinatura digital, utiliza um par de chaves diferentes, mas que se relacionam matematicamente, sendo uma a chave pública (utilizada para cifrar a mensagem) e a outra a chave privada (utilizada para decifrar a mensagem). O texto cifrado por uma chave pública só pode ser decifrado pela chave privada correspondente. A chave privada, portanto, deve ser de conhecimento apenas de seu titular, enquanto a chave pública deve ser conhecida por todos aqueles que queiram enviar uma mensagem codificada ao primeiro.

O processo inverso é utilizado na assinatura digital: o emissor, com sua chave privada, assina o documento e a conferência da assinatura pode ser feita por todos aqueles que possuem a chave pública correspondente. Essa operação será vista de forma mais detalhada no tópico relacionado à assinatura digital.

4.2. CRIPTOGRAFIA SIMÉTRICA

Na criptografia simétrica utiliza-se a mesma chave tanto para cifragem quanto para decifragem de uma mensagem ou documento (Figura 4.1). A cifragem é realizada através de operações de substituição, onde cada elemento (um bit, por exemplo) é mapeado em outro elemento, e transposições, nos quais os elementos são meramente trocados de posição.

A utilização de um algoritmo simétrico requer que a cifra seja forte o suficiente para que um terceiro seja incapaz de decifrar uma mensagem criptografada ou descobrir a chave. A tentativa de decifrar um texto cifrado a partir do conhecimento de características do texto original, ou até mesmo pares de textos claros e cifrados, é denominada de criptoanálise. Já a tentativa de utilizar todas as chaves possíveis em um texto cifrado até que o texto original

seja obtido é denominada de ataque de força bruta. Em média, metade do número de chaves disponíveis deve ser testado para se obter sucesso [25].

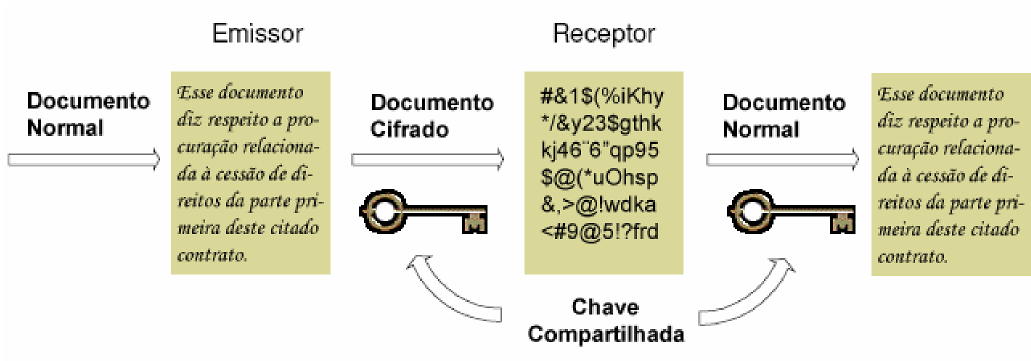


Figura 4.1 – Esquema simplificado de criptografia simétrica

O número de chaves possíveis para um algoritmo com chave de "n" bits é correspondente a 2^n e na média deve-se testar 2^{n-1} alternativas. Um algoritmo com tamanho de chave de 56 bits teria um espaço amostral de mais de 72 quatrilhões de possibilidades para a escolha da chave. A Tabela 4.1 mostra o tempo necessário para testar as chaves de acordo com o número médio de chaves possíveis, assumindo um computador que seja capaz de testar 1 milhão de chaves por segundo (10^6 testes/s) e 1 milhão de chaves por microssegundo (10^6 testes/µs) [25].

Tam chave (bits)	**Chaves possíveis/2**	**Tempo 10^6 testes/s**	**Tempo10^6 testes/µs**
32	2^{31}	35,8 minutos	2,15 milisegundos
56	2^{55}	1142 anos	10,01 horas
128	2^{127}	5,4 x 10^{24} anos	5,4 x 10^{18} anos
168	2^{167}	5,9 x 10^{36} anos	5,9 x 10^{30} anos

Tabela 4.1 – Tempo médio para teste de chaves com n bits

Um esquema de criptografia é dito computacionalmente seguro quando os dois critérios abaixo são satisfeitos [25]:

- O custo de "quebrar" a cifra excede o valor da informação criptografada;
- O tempo necessário para "quebrar" a cifra ultrapassa o tempo de vida útil da informação.

O DES (*Data Encryption Standard*), desenvolvido a partir de uma proposta da IBM no meio da década de 70, é um dos algoritmos simétricos mais conhecidos e utilizados. Utiliza-se de uma chave de 56 bits e tornou-se um padrão pelo *National Institute of Standards*

and Technology (NIST), sendo largamente adotado, até que há alguns anos, o seu uso foi desencorajado devido ao sucesso de ataques de força bruta pela tecnologia atualmente disponível. A fim de preservar o grande investimento em *software* e *hardware* feito para o DES, foi proposta uma variante, denominada 3DES, onde são utilizadas 3 chaves em uma operação sucessiva de cifragem, decifragem e cifragem, cada qual com uma chave diferente. O 3DES tem um comprimento de chave efetivo de 168 bits, o que torna praticamente inviável um ataque de força bruta. O 3DES mantém a compatibilidade com o DES, garantindo que não há método de criptoanálise disponível, mas têm como principal desvantagem ser mais lento se comparado com outros algoritmos atuais, principalmente para implementação em *software*.

Em razão dessas desvantagens, o NIST lançou em 1997 um concurso para selecionar um novo algoritmo para ser adotado como o AES - *Advanced Encryption Standard*, em substituição ao DES (e também ao 3DES) [26]. Encerrado o concurso em outubro de 2000 e publicado como padrão em novembro de 2001 (FIPS 197), o vencedor foi o algoritmo Rijndael[5], criado por dois recém doutores belgas, Joan Daemen e Vincent Rijmen. O Rijndael, assim como os outros finalistas (MARS, RC6, Twofish e o Serpent), são algoritmos com bloco de 128 bits e chaves de 128, 192 e 256 bits. Todos os algoritmos finalistas foram considerados seguros – o Rijndael seria o mais apropriado por motivos de eficiência e facilidade de implementação em equipamentos de recursos limitados (pouca memória e poder de processamento).

De modo geral, os algoritmos simétricos são executados muito mais rapidamente que os assimétricos. Na prática, para solucionar a questão da troca de chaves simétricas de forma segura, muitas vezes são utilizados em conjunto. Por exemplo, um algoritmo de chave pública é utilizado para cifrar uma chave gerada randomicamente e esta chave é usada para cifrar uma mensagem com um algoritmo simétrico. Esse esquema é muito comum ao se acessar uma página "segura" na internet, ou seja, onde as informações trocadas entre o navegador do cliente e o servidor são criptografadas através do protocolo SSL (*Secure Sockets Layer*).

4.3. CRIPTOGRAFIA ASSIMÉTRICA

A criptografia assimétrica, ao contrário da simétrica, utiliza um par de chaves: uma chave pública, que é utiliza para cifrar os dados, e uma correspondente chave privada

[5] Veja o anúncio do vencedor em http://www.nist.gov/public_affairs/releases/g00-176.htm

(secreta) para decifragem. Qualquer pessoa que tenha conhecimento da chave pública pode criptografar uma mensagem que somente o detentor da chave privada pode ler. Por isso, nos algoritmos assimétricos, as chaves são sempre geradas aos pares.

É computacionalmente inviável deduzir a chave privada a partir do conhecimento da chave pública. O conhecimento da chave pública permite a realização da operação de cifragem de uma mensagem, mas não permite que seja realizada a operação inversa de decifragem. A Figura 4.2 mostra um exemplo simples de cifragem e decifragem com a utilização das chaves pública e privada respectivamente.

O modo de operação da criptografia assimétrica resolve uma grande questão da criptografia de chave simétrica: permite que seja solucionado o problema de sigilo na troca de chaves e a também sua distribuição, uma vez que a chave utilizada para cifragem é a chave pública. Esse modo de operação nos permite obter a característica de confidencialidade fornecida pelos algoritmos simétricos. Entretanto, a criptografia simétrica pode ser utilizada de uma forma diferente, utilizando-se a chave privada para cifrar e a chave pública para decifrar. Isso é especialmente útil, pois garantindo-se o sigilo da chave privada, é possível termos um alto grau de certeza do autor da mensagem, pois o mesmo seria o detentor da chave privada. É essa característica que torna possível obter o requisito de autenticidade para um documento eletrônico.

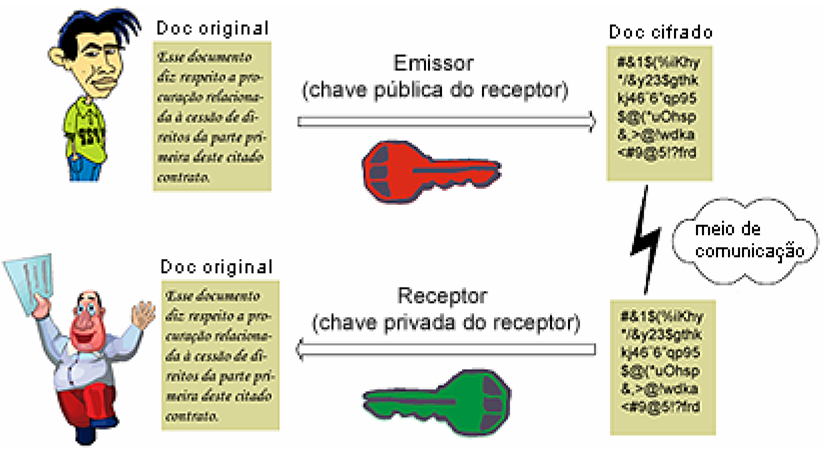


Figura 4.2 – Exemplo de criptografia assimétrica

O conceito de criptografia de chave pública foi apresentado pela primeira vez por Whitfield Diffie e Martin Hellman em 1976 no artigo denominado “*New Directions in Cryptography*” [19]. Esse trabalho revolucionou a pesquisa em criptografia, descrevendo os conceitos básicos da criptografia assimétrica e fornecendo um exemplo de algoritmo de troca

de chaves. Entretanto, embora o trabalho citasse a utilização de chaves públicas em assinaturas digitais, somente em 1977 três pesquisadores do MIT – Rivest, Shamir, Adleman implementaram um modelo matemático que foi publicado em 1978, e ficou mundialmente conhecido como algoritmo RSA (em referência as iniciais dos nomes de seus autores), sendo a base para a maioria das aplicações baseadas em criptografia assimétrica nos dias de hoje [20].

No algoritmo RSA, a chave pública é o produto de dois números primos grandes (pelo menos centenas de bits), selecionados aleatoriamente e a chave secreta é composta pelos próprios números primos. O algoritmo cifra usando o produto dos números primos e decifra utilizando os seus fatores. A segurança baseia-se na grande dificuldade matemática de se encontrar dois fatores primos de um número grande e assim inferir a chave privada a partir do conhecimento da chave pública. Não há método conhecido de fatoração que seja eficiente, a não ser verificando cada possibilidade individualmente [27].

O nível de segurança dos algoritmos assimétricos, em relação a um ataque de força bruta, também é diretamente relacionado ao tamanho das chaves. Entretanto, a criptografia utilizada no algoritmo RSA por exemplo, pode usar somente um subconjunto de todos os possíveis valores para uma chave de determinado tamanho. Assim pode-se inferir que o nível de segurança de um algoritmo de 128 bits na criptografia simétrica é maior que um algoritmo com chave de mesmo tamanho na criptografia de chave pública. Isso explica o fato de uma chave de 512 bits utilizada na criptografia assimétrica ser equivalente a uma chave de 64 bits na criptografia simétrica em relação ao esforço necessário ao ataque de força bruta (Tabela 4.2).

Criptografia Simétrica	**Criptografia Assimétrica**
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

Tabela 4.2 – Equivalência de chaves em um ataque de força bruta [28]

Embora a fatoração de números grandes seja um processo demorado e difícil, com os rápidos avanços na teoria dos números e o crescente poder computacional alguns sucessos tem sido alcançados. Em 1977, Ron Rivest, estimava que a fatoração de um número de 125 dígitos levaria 40 quatrilhões de anos. Em 1994, uma chave RSA de 129 dígitos foi fatorada em 8 meses, utilizando-se aproximadamente 5.000 MIPS/ano com a utilização de 1.600

computadores na Internet [31]. A Tabela 4.3 nos mostra o tempo estimado em MIPS/ano para fatorar determinados tamanhos de chave utilizadas em uma implementação do algoritmo RSA. Um MIPS/ano equivale a um computador executando 1 milhão de instruções por segundo durante um ano. Atualmente, recomenda-se a utilização de chaves de no mínimo 1.024 bits, sempre levando-se em consideração o tempo útil da informação e a viabilidade de implementação de chaves do maior tamanho possível.

Tam da chave	**MIPS/ano para fatoração**
512 bits	30.000
768 bits	200.000.000
1024 bits	300.000.000.000
2048 bits	300.000.000.000.000.000.000

Tabela 4.3 – Tempo estimado para fatoração de uma chave [28]

Na criptografia assimétrica a autenticidade é obtida com a criptografia da mensagem a ser enviada com a chave privada do emissor e a confidencialidade é obtida com posterior criptografia utilizando-se a chave pública do receptor. O receptor decifra a mensagem utilizando a sua chave privada (requisito confidencialidade) e depois utiliza a chave pública do emissor para obter a comprovação da autoria (requisito autenticidade).

Em síntese, em relação a assinatura de um documento eletrônico, a técnica de criptografia de chave pública permite que um emissor possa enviar dados “assinados” para um destinatário. Todos aqueles que possuem acesso a correspondente chave pública do emissor (que faz par com a chave privada utilizada na assinatura) podem verificar que o emitente é realmente o autor da assinatura aposta no documento.

5. ASSINATURA DIGITAL

5.1. INTRODUÇÃO

Conforme visto no capítulo anterior, a assinatura digital é o instrumento que fornece ao documento digital garantias, de tal modo que este possa ter força probante, ou seja, é um elemento de credibilidade do documento digital, que permite a conferência da autoria e da integridade do mesmo.

Deve-se observar que a assinatura digital é uma modalidade de assinatura eletrônica e não deve ser confundida com outros tipos de assinatura eletrônica, como a utilização de senhas, números PIN, autenticação biométrica ou quaisquer outros mecanismos que tenham o propósito de identificação, sem a utilização da criptografia assimétrica. A assinatura digital está relacionada diretamente ao uso de um par de chaves (chave pública e chave privada), normalmente associados a certificados digitais.

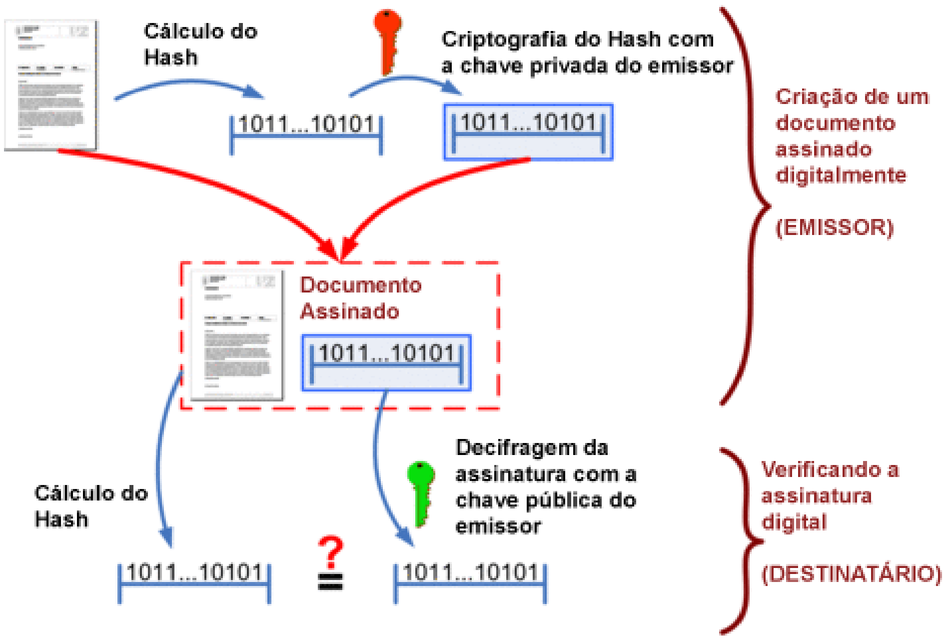


Figura 5.1 – Criando e verificando uma assinatura digital

A partir de um documento eletrônico e um software que permita a assinatura digital, utiliza-se um algoritmo de "*hashing*" onde é calculado um "resumo" do documento. Um algoritmo de "*hashing*" é uma função que gera uma saída de tamanho fixo (algumas dezenas de *bytes*) independentemente do tamanho da entrada. Com a chave privada do

emissor, esse "resumo" é criptografado e anexado ao documento eletrônico original tornando o mesmo um documento assinado digitalmente. O destinatário do documento, utilizando-se de software apropriado (que pode até pertencer ao sistema operacional) também efetua o cálculo do "resumo" do documento e o compara com a decifragem do hash anexado. Se os "resumos" não forem iguais, isso significa que o documento foi alterado após a sua assinatura ou a assinatura não foi gerada com a chave privada do pretenso emissor (Figura 5.1).

Cabe observar que a assinatura foi feita somente para o "resumo" e não para o documento todo. As duas razões principais são a necessidade de leitura do documento por qualquer pessoa (considerando que o documento não seja sigiloso) e a eficiência em razão do "resumo" ser uma pequena fração fixa de bits – normalmente 128 bits no algoritmo MD5 e 160 bits no caso de um dos algoritmos mais utilizados atualmente (SHA1).

5.2. FUNÇÕES DE HASHING

Uma função "*hash*", ou resumo, é uma função que tem como entrada uma mensagem de tamanho variável e como saída um resultado de tamanho fixo (normalmente de 128 a 512 bits). Uma função resumo pode ser usada para várias finalidades (encriptação, autenticação, classificação), mas um de seus usos mais típicos é para assinatura digital de documentos, arquivos e mensagens [29].

Para ter utilidade no processo de assinatura digital, a função de "*hashing*" deve ter as seguintes características [32]:

- ser relativamente fácil se computar o "*hash*" de uma mensagem permitindo implementações práticas em software e hardware;
- deve ser impraticável se determinar a entrada a partir de seu "*hash*" (função unívoca);
- deve ser impraticável se determinar uma outra entrada que resulte no mesmo "*hash*" de uma dada entrada (resistência a colisão);
- os valores de "*hash*" possíveis são estatisticamente equiprováveis;
- A saída da função "*hash*" deve possuir um tamanho fixo.

As funções de "*hashing*" mais utilizadas atualmente são a SHA1 (*Secure Hash Algorithm* – 1) e a MD5 (*Message Digest* – 5), ambas baseadas no algoritmo MD4, criado por Ron Rivest em 1990. Apesar de possuir um algoritmo muito eficaz e otimizado para plataformas 32 bits, a função MD4 foi rapidamente abandonada em razão da descoberta de

vulnerabilidades que permitiam explorar ataques de colisão no algoritmo, tornando o seu uso não apropriado para fins criptográficos [33].

Em 1991, a partir de melhorias no algoritmo MD4 incluindo novos passos e funções no algoritmo, foi lançado o seu sucessor denominado MD5. O MD5 gera um resumo de 128 bits, foi lançado como um Internet Standard (RFC 1321) e é largamente utilizado em aplicações de segurança e checagem da integridade de arquivos. Entre outras características, o algoritmo MD5 tem a propriedade de que cada bit do “resumo” ser função de cada bit na mensagem de entrada, o que aumenta o “efeito avalanche” da função – a mudança de um único bit, muda bastante o “*hash*” obtido na saída. A dificuldade de se encontrar duas mensagens com o mesmo “resumo” é da ordem de 2^{64} operações, enquanto que a possibilidade de encontrar uma mensagem dado o seu “resumo” é de 2^{128} [34].

Em 1993, o *National Institute of Standards and Technology* (NIST) propôs o algoritmo SHA (*Secure Hash Algorithm*) sendo publicado como padrão FIPS 180 em 1993 e revisado no FIPS 180-1 em 1995 e conhecido desde então como SHA-1. O algoritmo SHA (também denominado SHA0) e o SHA1 foram também baseados na função MD4 e ambos tem como principal vantagem a produção de um “*hash*” de 160 bits, tornando a dificuldade de se encontrar dois resumos iguais para a mesma mensagem da ordem de 2^{80} [25].

Em 1996, Hans Dobbertin anunciou ter encontrado uma colisão na função de compressão do MD5 [35] e em 1998 pesquisadores franceses encontraram colisões em ataques ao SHA0 [36], o que fez com que os criptógrafos recomendassem a utilização do SHA1 em lugar do MD5. Cabe ressaltar que a descoberta dessas colisões não necessariamente abre caminho para um ataque prático aos algoritmos, nem comprometem as aplicações que utilizam “*hashes*” criptográficos – como a utilização de assinaturas digitais – uma vez que não é possível forjar uma assinatura a partir de um documento pré-existente.

Mesmo assim, em 2001 o NIST propôs uma revisão do padrão FIPS 180-1, conhecido como FIPS 180-2 [37] e incluiu três novos algoritmos conhecidos genericamente como SHA2. Os algoritmos foram nomeados pelo tamanho de seu “*hash*” em bits: SHA-256, SHA-384 E SHA-512. Os algoritmos SHA-256 e SHA-512 são funções de “*hashing*” novas calculadas com “palavras” (“*word size*”) de 32 e 64 bits respectivamente. Elas utilizam deslocamentos e somas diferentes, mas a estrutura original do SHA0 foi mantida, diferindo apenas no número de iterações. O algoritmo SHA-384 é apenas uma versão truncada do SHA-512, não trazendo assim nenhuma vantagem em relação ao desempenho.

As novas funções de "*hashing*" denominadas SHA2 não foram avaliadas pelos criptógrafos da mesma forma que o algoritmo SHA1, mas como a estrutura e os detalhes dos algoritmos são bastante semelhantes, todos devem ter uma resistência a criptoanálise semelhante ao algoritmo SHA1, com dificuldade para se encontrar colisões bastante melhorada (2^{128}, 2^{192}, 2^{256} respectivamente para os algoritmos SHA-256, SHA-384, SHA-512).

Após a escolha do algoritmo Rijndael como o AES, Vincent Rijmen, um de seus autores em co-autoria com o brasileiro Paulo Barreto projetaram em 2000 um algoritmo de *hash* denominado WHIRLPOOL [38]. Esse algoritmo foi baseado em uma versão modificada do Square (um cifrador simétrico precursor do Rijndael) e utiliza operações matemáticas complexas denominadas "*substitution-permutation network*" (SPN). O WHIRLPOOL gera "resumos" de 512 bits que são tipicamente representados por 128 caracteres hexadecimais e foi também adotado pela ISO (*International Organization for Standardization*) e pelo IEC (*International Electrotechnical Commission*) (IEC) como padrão internacional ISO/IEC 10118-3.

5.3. ALGORITMOS DE ASSINATURA DIGITAL

Os dois principais algoritmos de assinatura digital são o RSA e o DSA, este último transformado em um padrão denominado DSS (*Digital Signature Standard*). O DSA foi inicialmente proposto pelo NIST para ser utilizado como o padrão de assinatura digital especificado no FIPS 186 em 1991. A última revisão do DSS foi proposta em 2000 e utiliza SHA1 como função "*hash*" e foi definida como FIPS 186-2. Espera-se o anúncio do FIPS 186-3 que possibilitará a utilização dos algoritmos de hashing SHA2 (SHA-256, SHA-384, SHA-512).

5.3.1. Algoritmo RSA

O RSA é um algoritmo que pode ser utilizado para cifragem, troca de chaves e assinatura digital. O funcionamento da assinatura de um documento utilizando o algoritmo RSA (Figura 5.2), segue os seguintes passos:

1. O documento ou mensagem a ser assinada (M) é submetido a função "*hash*" (H), produzindo um "resumo" de tamanho fixo.

2. Esse “resumo” é cifrado (E) com a chave privada do emissor (KRE), formando a assinatura propriamente dita.
3. A assinatura é anexada ao documento original e enviada ao receptor.
4. O receptor, a partir da mensagem recebida, calcula o “resumo” do documento utilizando a mesma função hash (H) do emissor.
5. A assinatura é decifrada (D) com a utilização da chave pública do emissor (KUE), obtendo-se o código hash que foi gerado pelo emissor
6. O receptor compara então o “resumo” que ele calculou com o “resumo” gerado pelo emissor da mensagem. Se ambos forem idênticos, a assinatura digital é válida e o documento é também considerado íntegro.

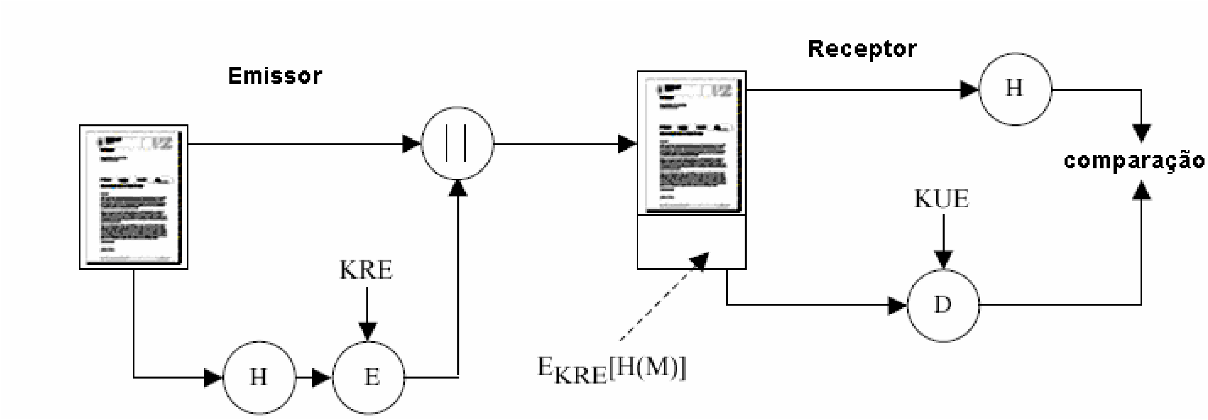


Figura 5.2 – Esquema de Assinatura RSA [25]

5.3.2. Algoritmo DSA

O DSA (*Digital Signature Algorithm)* é um algoritmo que utiliza o conceito de chave pública para gerar assinaturas digitais. O DSA utiliza como algoritmo de *hashing* o SHA e não pode ser usado para cifragem de dados. O funcionamento da assinatura de um documento utilizando o algoritmo DSA (Figura 5.3), é exemplificado abaixo:

1. O documento ou mensagem a ser assinada (M) é submetido a função hash (H), produzindo um “resumo” de tamanho fixo.
2. É gerado um número randômico (k), que em conjunto com o “resumo” (H), a chave privada do emissor (KRE) e a chave pública do receptor (KUR) são utilizados como entrada para a função de assinatura (ASS) que gera dois números denominados (r) e (s).
3. Os números (r) e (s), que podem ser considerados a assinatura propriamente dita, são anexados ao documento original e enviados ao receptor.

4. O receptor, a partir da mensagem recebida, calcula o "resumo" do documento utilizando a mesma função hash (H) do emissor.

5. O código hash (H) gerado mais os números (r) e (s) recebidos, a chave pública do emissor KUE e a chave pública do receptor KUR servem de entrada para a função de verificação de assinatura (VAS), que irá gerar um componente (r), o qual sendo igual ao componente (r) recebido comprova a validade da assinatura.

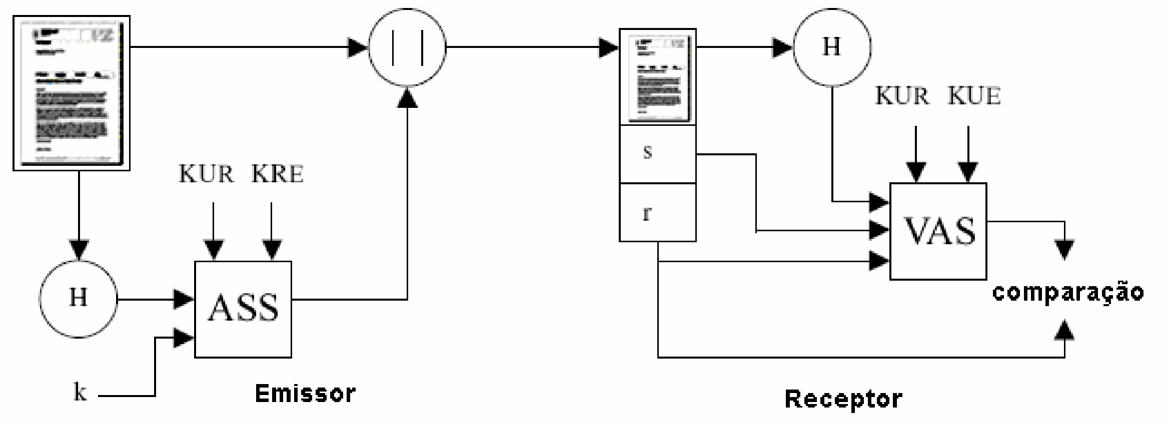


Figura 5.3 – Esquema de Assinatura DSS [25]

5.4. CARACTERÍSTICAS ESSENCIAIS

Segundo STALLINGS [25], utilizando-se qualquer tipo de assinatura digital, as seguintes propriedades tem que ser satisfeitas:

- Deve ser possível verificar o autor, data, e hora da assinatura.
- Deve ser possível autenticar o conteúdo na hora da assinatura.
- A assinatura deve ser prover condições de ser analisada por uma terceira parte com a finalidade de resolver disputas.
- O processo de produção, reconhecimento e verificação de uma assinatura digital deve ser relativamente simples.
- Não deve ser possível forjar uma assinatura.
- A assinatura efetuada deve ser baseada no conteúdo da mensagem.
- O armazenamento de uma assinatura digital deve ser possível.
- Não pode haver duas assinaturas idênticas.

Um dos mais importantes desdobramentos da descoberta da criptografia de chave pública é a sua utilização em assinaturas digitais. Entretanto, resta ainda uma questão em relação a utilização das chaves públicas: como confiar que determinada chave efetivamente pertence a um suposto emissor ? Para resolver esse problema, foi criada uma infra-estrutura denominada infra-estrutura de chaves públicas (ICP), ou seu acrônimo em inglês PKI (*Public Key Infrastructure*), que permite que os usuários sejam autenticados pelas suas respectivas chaves públicas através do uso de certificados digitais.

6. INFRA-ESTRUTURA DE CHAVES PÚBLICAS

As infra-estruturas de chaves públicas (ICP's) surgiram da necessidade de se autenticar as chaves públicas utilizadas para validação de assinaturas digitais. Deste modo, busca-se excluir a fragilidade do uso de sistemas que utilizam par de chaves para assinar documentos digitais no que se refere a confirmação de que aquelas chaves públicas que serão utilizadas para validar as assinaturas digitais são de fato de determinado signatário. O certificado digital é o instrumento utilizado para a validação das chaves públicas nestas estruturas, sendo ele próprio um documento digital, assinado digitalmente por uma autoridade certificadora, que contém diversos dados sobre o emissor e o titular do certificado, como nome do titular, identificação do algoritmo de assinatura, assinatura digital do emissor, validade do certificado, além da própria chave pública vinculada ao titular do certificado**.**

O Brasil criou a sua infra-estrutura de chaves-públicas, ICP-Brasil, através da Medida Provisória 2.220-2, de 24 de agosto de 2001. Esse capítulo aborda a criação e estruturação da ICP-Brasil, fornece os detalhes de um certificado digital e especifica as políticas e tipos de certificado emitidos pelas Autoridades Certificadoras da ICP-Brasil.

6.1. CERTIFICADOS DIGITAIS

6.1.1. Conceito

Um certificado digital nada mais é do que um documento eletrônico que contém a chave pública de um usuário (ou entidade) e dados de identificação do mesmo. Este documento deve ser assinado por uma autoridade confiável, denominada Autoridade Certificadora (AC), atestando sua origem e integridade [39]

Dessa forma, um certificado de chave pública (*Public-Key Certificate* – PKC) é um conjunto de dados que fornece um método confiável para distribuição de chave pública entre usuários que utilizam serviços de criptografia e assinatura digital. Ao se obter a chave pública de um usuário em uma AC confiável e verificando-se a assinatura contida no certificado, pode-se ter certeza de que a chave realmente pertence ao pretenso usuário, e que somente ele dispõe da correspondente chave secreta que o capacita a decifrar mensagens cifradas com aquela chave pública, ou assinar documentos com a correspondente chave privada.

O X.509 é o padrão mais utilizado para certificados digitais definido pelo ITU-T (*International Telecommunication Union*) com características que permite a inclusão de pares nome/valor no certificado padrão. Um certificado X.509, permite entre outras informações possíveis, os seguintes dados de identificação (Figura 6.1):

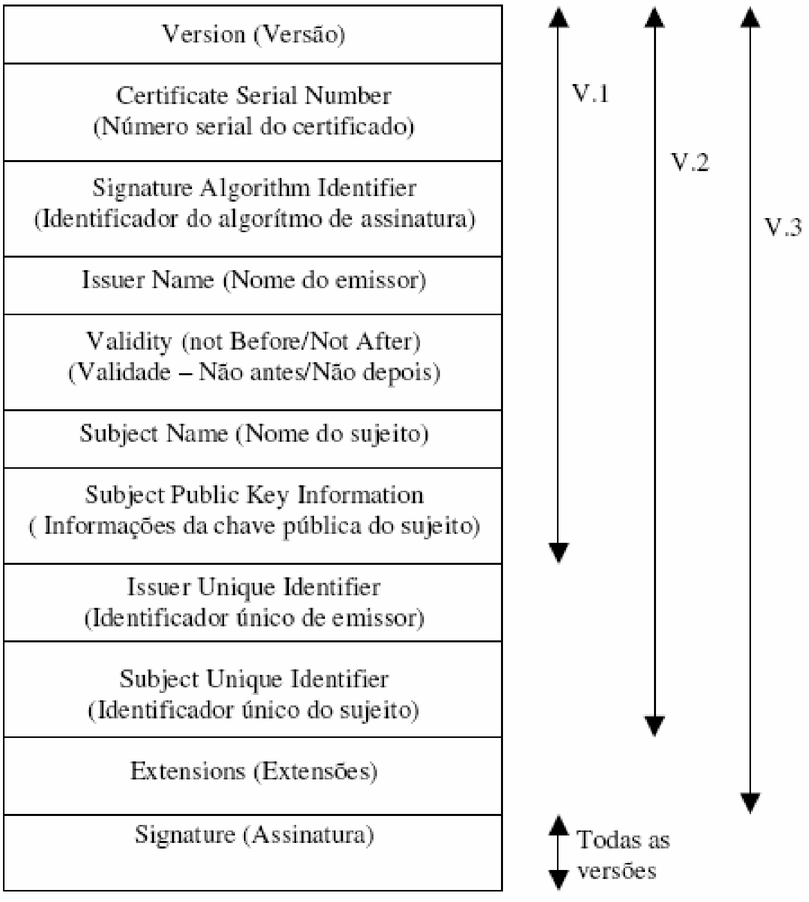


Figura 6.1 – Estrutura de um certificado X.509 nas versões 1, 2 e 3 [40]

Versão: identifica a versão do certificado padrão X.509 (versão 1,2 ou 3).

Número serial do certificado: valor numérico único atribuído pela AC.

Identificador de algoritmo de assinatura: informa o algoritmo e parâmetros utilizados para assinar o certificado.

Nome do emissor: nome da AC que criou e assinou o certificado.

Validade (Não antes/Não depois): período de validade do certificado, inicio e fim.

Nome do sujeito: nome do usuário ou entidade a quem este certificado se refere.

Informações sobre a chave pública do sujeito: a chave pública do sujeito ou entidade, junto com a identificação do algoritmo com o qual esta chave pode ser usada.

Identificador único do emissor: elemento usado para identificar se a AC emissora é única.

Identificador único do sujeito: elemento usado para identificar se o sujeito é único.

Extensões: conjunto de uma ou mais informações de extensão. As extensões foram implementadas na versão 3.

Assinatura: elemento que protege todos os outros campos do certificado. Contém o código *hash* dos outros campos, cifrado com a chave privada da AC, e a identificação do algoritmo de assinatura.

6.1.2. Classes de Certificados

As Autoridades Certificadoras (ACs) podem ser privadas (institucionais, por exemplo) comerciais ou até mesmo emitir certificados gratuitos. A vantagem da utilização de uma AC comercial é a confiança depositada pelo grande número de usuários que a utilizam, além do fato de que os certificados emitidos têm validade externa, fora do âmbito de uma única instituição.

A Verisign é uma das primeiras e mais conhecidas Autoridades Certificadoras comerciais no mundo e surgiu a partir da americana RSA Security em 1995. No Brasil, a Certisign é uma subsidiária da Verisign, sendo hoje líder na América Latina em certificação digital. A Verisign instituiu o conceito de três classes de certificados digitais [41].

Os Certificados Digitais Classe 1 são emitidos apenas para indivíduos. Tais Certificados confirmam apenas a existência de um endereço de correio eletrônico, permitindo a troca de mensagens de forma segura. Em geral, os Certificados Classe 1 são gratuitos, não sendo utilizados para fins comerciais ou outros fins em que seja requerida a prova de identidade do assinante.

Os Certificados Digitais Classe 2 podem ser fornecidos a uma pessoa física ou um indivíduo pertencente a uma instituição (pessoa jurídica). Os Certificados de Classe 2 confirmam que as informações de solicitação fornecidas pelo assinante (correio eletrônico, número da identidade e endereço) não entram em conflito com as informações de bancos de dados reconhecidos (no Brasil podemos citar a SERASA e o SPC) e no caso de uma pessoa jurídica, uma autoridade de registro (AR) é quem autentica a identidade do usuário. Tem confiabilidade superior aos certificados classe 1, pois oferece garantias razoáveis da identidade de um assinante, porém não à prova de erros. Permitem a realização de operações de baixo risco, como correio eletrônico, validação de software e pequenas transações onde se exige o mínimo de prova da identidade do assinante.

Os Certificados Digitais Classe 3 também são emitidos para pessoas físicas ou jurídicas. Oferecem garantias importantes com relação à identidade de assinantes individuais, pois exigem que compareçam pessoalmente perante uma AR de Classe 3 ou seu

representante. Em relação a pessoa jurídica, oferece garantias em relação à existência e ao nome de organizações dos setores público ou privado e inclui a análise, por parte da AR pertinente de Classe 3, dos registros de autorização fornecidos pelo assinante ou por bancos de dados reconhecidos de terceiros. Como os Certificados Digitais Classe 3 exigem a comprovação de documentos de forma presencial e uma análise mais rígida dos dados apresentados, estes são os certificados de maior confiabilidade. São normalmente utilizados em transações de comércio eletrônico, intercâmbio eletrônico de dados (EDI), transações bancárias e serviços on-line onde é necessária a comprovação da identidade dos participantes.

6.1.3. Fases de um certificado digital

Um certificado digital passa por várias fases, desde o seu requerimento até o fim de sua validade. A Autoridade Certificadora é responsável pelo acompanhamento de todo o ciclo de vida dos certificados por ela emitidos. O ciclo de vida de um certificado é constituído das seguintes etapas [42]:

a) Requerimento: é o pedido de expedição do certificado, feito pela pessoa interessada junto à Autoridade Certificadora;

b) Validação do Requerimento: é função da Autoridade Certificadora garantir que o requerimento seja válido e que os dados do requerente estejam corretos;

c) Emissão do Certificado: é o ato de reconhecimento do título do certificado digital pelo requerente e sua emissão;

d) Aceitação do Certificado pelo requerente: após emitido, o requerente deve retirá-lo da Autoridade Certificadora e confirmar a validade do certificado emitido;

e) Uso do Certificado: é o período em que o certificado pode ser utilizado, sendo seu uso de total responsabilidade do requerente;

f) Suspensão do certificado digital: é o ato pelo qual o certificado se torna temporariamente inválido para operações por algum motivo especificado pela Autoridade Certificadora, como por exemplo, o comprometimento da chave pública;

g) Revogação do certificado: é o processo pelo qual o certificado se torna definitivamente inválido pelo comprometimento da chave privada do titular ou, ainda, quando ocorrer algum fato que torne o certificado digital inseguro para uso. Um certificado suspenso ou revogado deve ser publicado na Lista de Certificados Revogados (LCR) e estar sempre disponível para consulta;

h) Término da validade e renovação do Certificado: o Certificado Digital tem um período pré-estabelecido de validade atribuído pela Autoridade Certificadora. Normalmente, este período é de um a três anos, dependendo do tipo e finalidade do certificado.

6.1.4. Armazenamento de certificados e chaves

Uma vez gerado um certificado digital e as suas correspondentes chaves (privada e pública), os mesmos devem ser apropriadamente armazenados. Como se tratam de arquivos digitais, a forma mais comum é a utilização de qualquer tipo de mídia de armazenamento de dados, inclusive o disco rígido do computador. As mídias mais comuns são as seguintes:

- Mídia magnética: Disquete
- Mídia óptica: CD-ROM, CD-R, CD-Card (25 Mb)
- “*Smart card*” ou cartão inteligente
- “*Token*” de armazenamento
- Chips de memória diversos (“*pen drive*”, “*memory card*”)

Em razão da importância da guarda da chave privada, deve-se evitar armazená-la no disco rígido do computador, preferindo o uso de dispositivos móveis. Caso a chave seja armazenada no disco rígido (normalmente os certificados mais simples do tipo 1 permitem essa possibilidade) é imprescindível que a mesma seja protegida por criptografia ou utilize-se de um repositório específico, como o “*Cryptographic Services Provider*” da Microsoft, que mantém os dados em sigilo e permite a exportação e importação de certificados e chaves.

Entretanto, os meios mais seguros de armazenamento são os “*smart cards*”, que possibilitam que o par de chaves seja gerado dentro do cartão não permitindo a exportação ou qualquer outro tipo de reprodução ou de cópia da chave privada. Um “*smart card*” é um cartão semelhante a um cartão de crédito que contém um microprocessador e uma unidade de memória que armazenada e recupera dados através de vários mecanismos de segurança (criptografia, restrição ao acesso indevido dos dados armazenados, inviolabilidade, etc). Deve ser utilizado com uma leitora de cartões específica e por isso tem um custo relativamente elevado.

Os “*tokens*” também são dispositivos de armazenamento importantes, muitos já funcionando como um “*smart card*” com a vantagem de não necessitar de uma leitora específica de cartão, uma vez que são alimentados e conectados diretamente à porta USB do computador. Os “smart cards” em conjunto com os “*tokens*” inteligentes são dispositivos

ideais para o armazenamento e utilização dos certificados digitais de classe 3, uma vez que possuem mecanismos de segurança para armazenamento e uso seguro da chave privada de um usuário ou entidade (Figura 6.2).



Figura 6.2 – Dispositivos de armazenamento removível

6.2. ICP-BRASIL

A ICP-Brasil pode ser definida como um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública [43]. Tem como objetivo garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras [44].

6.2.1. Estrutura Básica

A Medida Provisória 2.220-2, de 24 de agosto de 2001, criou a sua infra-estrutura de chaves-públicas – ICP-Brasil. Essa medida visa garantir a validade jurídica aos documentos eletrônicos assinados digitalmente com o uso dos certificados digitais emitidos por Autoridades Certificadoras credenciadas e homologadas na ICP-Brasil.

A MP 2.200-2, embora sem definir a organização da ICP-Brasil, indicou antecipadamente os órgãos que a compõem, na seguinte ordem: um Comitê Gestor (autoridade gestora das políticas de certificação), a Autoridade Certificadora Raiz (AC-Raiz), as Autoridades Certificadoras (ACs) e as Autoridades de Registro (ARs). Uma estrutura genérica de representação da ICP-Brasil pode ser vista na Figura 6.3.

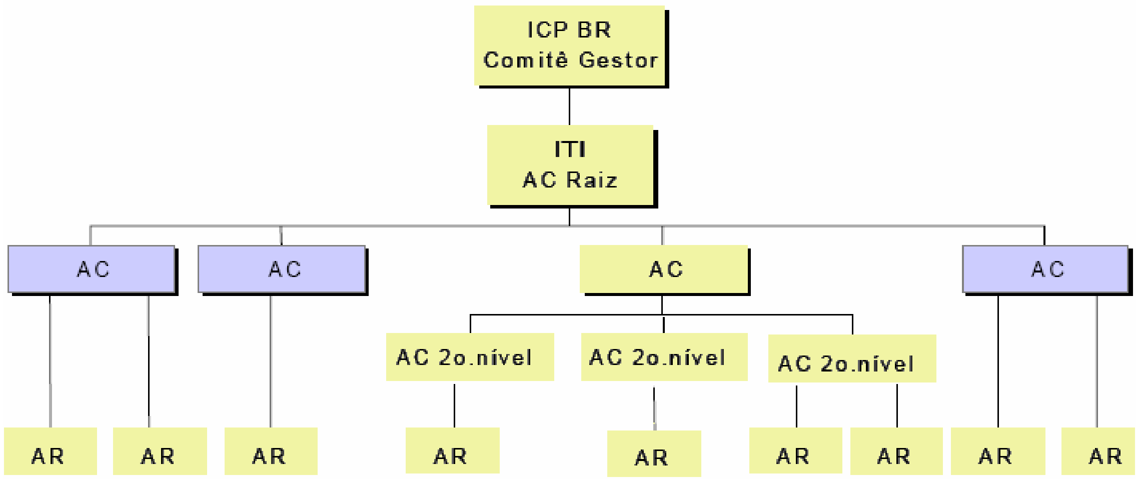


Figura 6.3 – Estrutura genérica da ICP-Brasil

O Comitê Gestor é o órgão que exerce a função de autoridade gestora das políticas de certificação da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil integrantes de setores interessados, designados pelo Presidente da República, e representantes de diversos órgãos governamentais. A coordenação do Comitê Gestor da ICP-Brasil é exercida pelo representante da Casa Civil da Presidência da República.

A Autoridade Certificadora Raiz é a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. O papel de Autoridade Certificadora Raiz da ICP-Brasil é desempenhado pelo ITI – Instituto Nacional de Tecnologia da Informação, autarquia federal vinculada ao Ministério da Ciência e Tecnologia. A ela compete [44]:

a) emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu;

b) gerenciar a lista de certificados emitidos, revogados e vencidos;

c) executar atividades de fiscalização e auditoria das ACs e das ARs e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil;

d) exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

As Autoridades Certificadoras (ACs) são as entidades componentes da cadeia de certificação responsáveis pela emissão de certificados digitais a usuários finais. Situam-se em

nível inferior ao da AC-Raiz na cadeia de certificação, já que são credenciadas por esta última para emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular (usuário final). A essas autoridades certificadoras (as ACs), compete basicamente [44]:

a) emitir, expedir, distribuir, revogar e gerenciar os certificados;
b) colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes;
c) manter registro de suas operações.

As Autoridades de Registro (ARs) são entidades operacionalmente vinculadas a uma determinada AC. Em outras palavras, cada AC opera através de uma AR, para efeito de realizar a tarefa de identificação e cadastro dos usuários finais. Além de cadastrar e identificar usuários, as ARs encaminham solicitações de certificados às ACs e devem manter registros de suas operações. Qualquer pessoa, de direito público ou privado, desde que preenchendo os requisitos gerais da política de certificação da ICP-Brasil, pode requerer credenciamento como uma Autoridade Certificadora ou uma Autoridade de Registro.

A decisão do Governo Brasileiro de implantar uma Infra-Estrutura de Chaves Públicas decorreu da necessidade de regulamentar a questão da certificação digital, considerando a disseminação do uso da tecnologia da informação na sociedade.

Estudos foram desenvolvidos para escolha da solução técnica de implantação da ICP-Brasil, os quais levaram em consideração as experiências desenvolvidas na normalização e padronização internacionais adotadas por diversos países, assim como o sistema político adotado no Brasil, as características sociais, culturais, administrativas e técnicas observadas em outros projetos do Poder Executivo Federal [45].

Uma das principais características da ICP-Brasil é sua estrutura hierárquica. No topo da estrutura, encontra-se a Autoridade Certificadora Raiz e, abaixo dela, estão as diversas entidades. O contrato de adesão é subordinado a um processo de credenciamento, no qual são analisadas a capacidade jurídica, econômico-financeira, fiscal e técnica de cada entidade. Também é exigida a contratação de seguro de responsabilidade civil e a realização de auditorias prévias e anuais. Tudo isso tem o objetivo de garantir a segurança do processo, desde a identificação dos titulares até a emissão dos certificados, trazendo, assim, confiabilidade a toda estrutura e aos atos praticados em seu âmbito [46].

A geração, distribuição e gerenciamento das chaves públicas e dos certificados digitais é feita por meio das autoridades certificadoras (ACs). São essas autoridades certificadoras que vão garantir, por exemplo, que uma chave pública ou certificado digital

pertence realmente a uma determinada empresa ou pessoa. São elas que formam a cadeia de confiança que dá segurança ao sistema. Fazem o papel desempenhado pelos notários no sistema de certificação tradicional. Da mesma forma que os cartórios tradicionais, são organizadas segundo critérios legais e obedecem, na prestação dos seus serviços de certificação, a toda uma política de procedimentos, padrões e formatos técnicos estabelecidos em regimes normativos. Obedecem, portanto, a um modelo técnico de certificação e estrutura normativa, que define quem pode emitir certificado para quem e em quais condições.

Exemplos de algumas entidades cadastradas como Autoridades Certificadoras na ICP-Brasil são: a Caixa Econômica Federal, a Certisign, a Presidência da República, a Secretaria da Receita Federal, o Serasa e o Serpro [46].

6.2.2. Certificados emitidos pela ICP-Brasil

De acordo com as atuais políticas de certificado adotadas no âmbito da ICP-Brasil, são 8 os tipos de certificado emitidos para usuários finais, sendo 4 relacionados com assinatura digital (A1, A2, A3 e A4) e 4 com sigilo (S1, S2, S3, S4). Os números associados aos tipos de certificados (1 a 4) definem uma escala de segurança, onde os tipos A1 e S1 estão associados aos requisitos menos rigorosos e os tipos A4 e S4 aos requisitos mais rigorosos [47].

Os certificados de tipos A1, A2, A3 e A4 são utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações. Os certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo. Certificados de quaisquer dos tipos relacionados acima, de assinatura ou de sigilo, podem, conforme a necessidade, ser emitidos pelas ACs para pessoas físicas, pessoas jurídicas, equipamentos ou aplicações.

A Tabela 6.1 resume as características principais dos certificados, informando respectivamente o tipo de certificado, o tamanho da chave em bits, o processo de geração das chaves, como é feito o armazenamento da chave, a validade máxima do certificado, a freqüência em horas da emissão da Lista de Certificados Revogados (LCR) e o tempo limite em horas para a revogação de um certificado.

Os certificados do tipo A1 podem ser armazenados no próprio disco rígido do computador, em mídias simples como um disquete ou CD-ROM e permitem que as chaves privadas possam ser exportadas ou importadas de seu local original. Os modelos A2, A3 e A4 exigem que as chaves sejam geradas internamente sem possibilidade de exportação ou importação. Portanto, dentre os modelos apresentados, é possível destacar os tipos A3 e A4 como os modelos mais seguros, pois armazenam as chaves privadas em cartões inteligentes ou "*tokens*" com capacidade de geração de chave, o que quer dizer que a chave é gerada dentro do dispositivo, não havendo necessidade de ficar exposta .

Tipo Cert.	**Chave Criptográfica**			**Validade**	**Freq. LCR**	**Limite Revog.**
	Tamanho	**Geração**	**Armazenamento**			
A1 e S1	1024 bits	Software	Repositório protegido por senha e/ou identificação biométrica, cifrado por software	1 ano	6 h	12 h
A2 e S2	1024 bits	Software	Cartão Inteligente ou Token, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica	2 anos	6 h	12 h
A3 e S3	1024 bits	Hardware	Cartão Inteligente ou "*token*", ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica ou hardware criptográfico aprovado pelo CG da ICP-Brasil	3 anos	6 h	12 h
A4 e S4	2048 bits	Hardware	Cartão Inteligente ou "*token*", ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica ou hardware criptográfico aprovado pelo CG da ICP-Brasil	3 anos	6 h	12 h

Tabela 6.1 – Comparativo de Requisitos Mínimos por Tipo de Certificado [47]

Esse capítulo abordou as características e tipos de um certificado digital e de uma Infra-Estrutura de Chaves Públicas, em particular da ICP-Brasil. Em conjunto com os capítulos 4 (Criptografia) e 5 (Assinatura Digital) esses esclarecimentos encerram o entendimento das questões técnicas que permitem o uso adequado da certificação digital. O próximo capítulo apresentará uma análise crítica relacionada a essas questões técnicas, bem como irá tratar da legislação brasileira e das questões legais relacionadas ao uso dos certificados digitais. Será apresentado também um sucinto resumo da situação das leis relacionadas à certificação digital e assinatura digital existentes em outros países.

7. NORMALIZAÇÃO E REGULAMENTAÇÃO LEGAL

Deve-se levar em conta que os avanços tecnológicos de uso comum pela sociedade muitas vezes levam tempo até serem absorvidos pelo Direito. A legislação que trata dos documentos eletrônicos apenas começou a surgir em meados da década passada. Era de se esperar que os países de maior renda fossem os primeiros a legislar sobre o tema, uma vez que são também eles os que fazem uso mais intenso da tecnologia. Esse capítulo cita as principais legislações estrangeiras relacionadas à assinatura digital, apresenta os principais conceitos dos elementos básicos do processo legislativo brasileiro e enumera a legislação pertinente aos documentos eletrônicos e à assinatura digital, inclusive aquelas ainda em tramitação no Congresso Nacional.

7.1. LEGISLAÇÃO ESTRANGEIRA

Em 1995, no estado de Utah – Estados Unidos, surge a primeira norma a respeito de documentos e assinaturas digitais (*Utah Digital Signature Act* [48]), notabilizada não só pela precedência como pelo detalhamento técnico nela contido. O objetivo principal da legislação da assinatura digital do estado de Utah é de promover o desenvolvimento de uma infra-estrutura de chave-pública. Na legislação vigente no estado de Utah são detalhados os direitos e as responsabilidades das partes em uma transação que utilize a criptografia de chave pública.

A importância de se regularizar a assinatura digital tornou-se ainda mais expressiva quando, em 1996, a União Européia adotou a lei da Comissão das Nações Unidas sobre o Direito do Comércio Internacional (*United Nations Commission on International Trade Law* – UNCITRAL [49]), que se tornou uma lei modelo sobre o comércio eletrônico, que serviria de referencial aos países-membro. Segundo BURNETT [40], "a lei modelo UNCITRAL é de alto nível, permitindo um método para as assinaturas e registros eletrônicos sem nenhuma menção quanto às assinaturas digitais ou à criptografia".

Desde então outros estados norte-americanos passaram a buscar a regulamentação do uso de assinaturas digitais, como as normas dos estados da Califórnia (*Digital Signature Regulations* [50]), de Illinois (*Electronic Commerce Security Act* [51]), e da Georgia (*Electronic Records and Signature Act* [52]). Em 2000, o então presidente dos EUA, Bill Clinton, sancionou o *Electronic Signatures in Global and National Commerce Act* [53], lei

que regula assinaturas eletrônicas e visa facilitar o uso de documentos eletrônicos e assinaturas eletrônicas nas transações comerciais entre Estados e países. Essa nova lei inclui, dentre outros, vários pontos importantes como definição de escopo, aplicação, direitos do consumidor, validade de assinaturas eletrônicas, contratos e arquivos eletrônicos e regras para autenticação de documentos.

Na Europa, diversos países também já adotaram leis que tratam dos documentos e assinaturas digitais: Alemanha (*Gesetz zur digitalen Signatur* [54]), Itália (*Decreto del Presidente della Repubblica*, nº 513, 1997 [55]), Inglaterra (*Electronic Communications Act, 2000* [56]), França (*Loi n°2000-230, 2000* [57]), Portugal (*Decreto-Lei n.º 290-D, de 2 de Agosto 1999* [58]). Deve-se destacar a Diretiva 1999/93/EC [59] do Parlamento Europeu, que tem por objetivo nortear as nações européias no que se refere à produção legislativa a respeito de documento e assinatura digital, uma vez que normas divergentes poderiam significar barreiras à integração entre os países membros.

Na América do Sul, além do Brasil, outros países também disciplinam a questão dos documentos e assinaturas digitais. Por exemplo, o Chile o faz por meio do *Decreto Supremo n. 81 de 1999* [60] , a Colômbia mediante *a Ley 527 de 1999* [61] e a Argentina com o *Decreto 427 de 1998* [62].

O Anexo II, apresenta uma análise comparativa entre a legislação adotada em vários países e também por organismos internacionais.

7.2. LEGISLAÇÃO BRASILEIRA

É necessária uma pequena introdução ao processo legislativo brasileiro com o objetivo de esclarecer o significado de seus elementos básicos, que são utilizados nesse trabalho. Uma das principais funções do Congresso Nacional e de suas casas – Câmara dos Deputados e Senado Federal – é a de elaborar normas legais. Trata-se do processo legislativo que compreende de acordo com o art. 59 da CF (Constituição Federal), a elaboração de emendas à constituição, leis complementares, leis ordinárias, leis delegadas, medidas provisórias, decretos legislativos e resoluções [63]. A Figura 7.1 mostra um fluxo do processo legislativo. De maneira simplificada, após a iniciativa é criada uma proposição – normalmente um projeto de lei – na Câmara ou no Senado. Durante a apreciação pela casa criadora, a proposição passa por várias comissões podendo sofrer emendas e substitutivos. Se aprovada, segue para a outra casa (revisora) onde tramita da mesma forma e obtendo parecer favorável, vai para a sanção presidencial e posterior publicação; se houver veto do Presidente da

República, o congresso pode mantê-lo ou rejeitá-lo. Se o Congresso rejeitar o veto, o Presidente deve promulgar a lei que seguirá então para publicação.

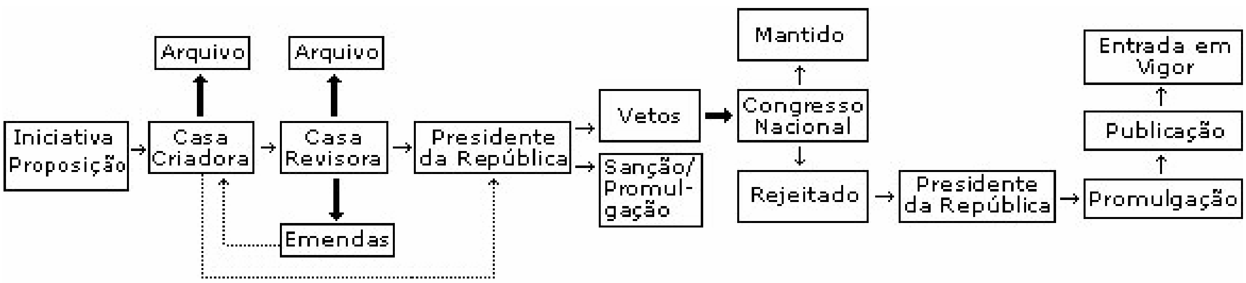


Figura 7.1 – Fluxo simplificado do Processo Legislativo [64]

A seguir serão apresentados os conceitos dos elementos básicos do Processo Legislativo, bem como os principais decretos, medidas provisórias e projetos de lei relacionados ao tema documento eletrônico e assinatura digital no Brasil.

7.2.1. Elementos do Processo Legislativo

Uma proposição é toda a matéria sujeita a deliberação em uma das casas do Congresso Nacional (Câmara dos Deputados ou Senado Federal) e dependendo de sua natureza ou de quem a inicie, a proposição deve ser apresentada no Plenário, nas Comissões ou na Mesa Diretora [63].

Um projeto de lei (PL) destina-se a regular as matérias de competência do Poder Legislativo, com a sanção do Presidente da República. Com a legislação atual, um projeto de lei pode ter sua tramitação iniciada tanto na Câmara dos Deputados como no Senado Federal, devendo ser avaliado e aprovado por ambos.

As emendas constitucionais (EC) são manifestações do poder constituinte derivado que visam a reformar parcialmente a constituição, através de acréscimos, modificações ou supressões das normas constitucionais [65]. É a forma encontrada pelo poder constituinte para atualizar a constituição de acordo com os novos tempos e adaptá-las às necessidades e conveniências do povo, sem necessidade de se fazer uma nova constituição por inteiro. A proposta de emenda será discutida e votada em cada casa do Congresso Nacional, em dois turnos, considerando-se aprovada se obtiver, em ambos, três quintos dos votos dos respectivos membros.

O direito brasileiro conhece três espécies de leis, que são as ordinárias, as complementares e as delegadas. Lei, segundo QUEIROZ [66], é o ato normativo de caráter

geral e abstrato elaborado pelo poder competente, por seu órgão, de acordo com o procedimento previsto na CF. É também um corpo de regras para a direção da conduta humana, que é imposto e ministrado aos cidadãos de um dado Estado. A apresentação ou proposição de um projeto de lei complementar ou ordinária pode, em princípio, ser feita por qualquer Deputado ou Senador, por comissão da Câmara, do Senado ou mista, pelo Presidente da República, pelo Supremo Tribunal Federal e demais tribunais, pelo Procurador Geral da República e pelo povo, o que se denomina de "iniciativa popular".

A lei complementar, como o próprio nome diz, é o diploma legal destinado a complementar a CF [67]. As matérias que devem ser regulamentadas através de lei complementar se encontram taxativamente previstas na Constituição. O projeto de lei complementar deverá ser discutido e votado em um único turno de votação, tendo por quorum a maioria absoluta, ou seja, mais da metade do total de membros integrantes da Casa.

Uma lei ordinária é assim denominada no processo legislativo para distingui-la da lei complementar ou delegada, já que, na prática, é denominada simplesmente lei [68]. O campo material por elas ocupado é residual, ou seja, tudo o que não for regulamentado por lei complementar, decreto legislativo e resoluções. O projeto de lei ordinária deverá ser discutido e votado em um único turno de votação, tendo por quorum a maioria simples, ou seja, mais da metade dos membros presentes à sessão de votação.

A lei delegada reflete a moderna tendência do Direito Público, quanto à admissibilidade de o Legislativo delegar, ao Presidente da República, poderes para elaboração de leis em casos expressos [69]. Tem por objetivo dar os instrumentos para o Presidente adotar certos mecanismos que a lei permite. Deve ser solicitada por resolução ao Congresso Nacional e, esta fixa seus limites, bem como, se haverá ou não a apreciação do projeto de lei delegada pelo Congresso Nacional. Havendo apreciação, o Congresso Nacional a fará em votação única, sendo vedada qualquer emenda.

A Medida Provisória (MP) é o ato normativo praticado pelo Presidente da República, quando se apresentam situações emergenciais e relevantes, possuindo por isso, força de lei. Atualmente seu prazo de vigência é de sessenta dias; prorrogável, nos termos do § 7o do art. 62 da CF, uma vez por igual período, devendo o Congresso Nacional disciplinar, por decreto legislativo, as relações jurídicas delas decorrentes, quando a medida provisória for rejeitada [63]. A MP substituiu o antigo decreto-lei e somente o Presidente da República é legitimado a editá-la, sob os pressupostos jurídicos de relevância e urgência.

As Medidas Provisórias estiveram submetidas a dois regimes constitucionais distintos desde a promulgação da Constituição Federal de 1988. O primeiro regime vigorou da promulgação da Constituição até a data da promulgação da Emenda Constitucional n° 32/2001, de 11 de setembro de 2001 [70]. Nesse primeiro regime, as medidas provisórias possuíam uma eficácia inicial de apenas trinta dias, mas podiam ser sucessivamente reeditadas pelo Presidente da República, mantendo-se a regulação da matéria com força de lei enquanto houvesse reedição. O segundo regime, atualmente em vigor, foi implantado pela EC de nº 32/2001 e, portanto, somente é aplicável às medidas provisórias editadas a partir da promulgação dessa emenda constitucional.

Porém, na data da promulgação da EC nº 32/2001 havia no Congresso Nacional sessenta e seis medidas provisórias antigas em tramitação, ou seja, editadas no regime constitucional anterior, antes de 11/09/2001. Foi necessário estabelecer uma regra especial para essas medidas provisórias, e esse papel foi cumprido pelo art. 2º da EC nº 32/2001, nos seguintes termos: "As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional" [70].

Enquanto não ocorrer uma dessas hipóteses, essas medidas provisórias continuarão regulando, com força de lei, as matérias nelas tratadas, independentemente de qualquer ato. Não há que se falar em necessidade de reedição, de prorrogação de prazo etc., pois o próprio art. 2º da EC nº 32/2001 já lhes outorgou vigência por prazo indeterminado. Em especial, esse é o caso da MP 2.200-2, de 24 de agosto de 2001 disciplina o uso dos documentos e assinaturas digitais e que continua válida até os dias de hoje.

O decreto legislativo é o instrumento normativo através do qual são materializadas as competências exclusivas do Congresso Nacional. Além das matérias enumeradas na Constituição Federal, o Congresso Nacional deverá regulamentar, por decreto legislativo, os efeitos decorrentes da medida provisória não convertida em lei conforme já citado anteriormente [71].

Já o conceito de resolução vem do latim "*resolutione*" – resolver, deliberar, romper, rescindir. É empregado em várias acepções, normalmente indicando deliberação ou determinação. Versa sobre matéria de exclusiva competência no âmbito de um Poder, não estando subordinada nem sujeita à aprovação ou referendo de qualquer outro. Dizem respeito a questões de ordem administrativa, legislativa ou administrativa e de competência privativa de um órgão, como por exemplo a regulamentação de matérias de competência da Câmara dos

Deputados e do Senado Federal [72]. O processo de elaboração das resoluções será disciplinado pelos regimentos internos dos órgãos, em face de o texto constitucional ser omisso a respeito.

Não sendo considerado integrante do processo legislativo propriamente dito, temos ainda o decreto emanado do Poder Executivo. O decreto é considerado um ato administrativo, com o fim de regulamentar a lei propriamente dita, ou de ensejar, a determinado Poder, a realização dos atos inerentes à sua competência. O decreto pode ser autônomo ou regulamentar. Autônomo, quando versa matéria ainda não tratada, especificamente, por alguma lei, suprindo portanto, omissões do direito positivo. Não pode, evidentemente, cuidar de matérias que somente por lei possam ser disciplinadas. Já o decreto regulamentar ou de execução é aquele que tem por objetivo explicar o conteúdo da lei e facilitar sua execução [73].

7.2.2. Projetos de lei, Decretos e Medidas Provisórias no Brasil

Nesta seção serão apresentados os principais decretos, medidas provisórias e projetos de lei que tratam da normalização de documentos eletrônicos, assinaturas eletrônicas e formas de viabilizar a sua utilização. Pela importância em que representaram no momento de sua publicação, também serão apresentados alguns decretos que já foram revogados, em razão de terem servido de base para proposições subseqüentes.

Diante da intensificação do uso de microcomputadores na Administração Pública e como conseqüência direta o crescimento vertiginoso de documentos eletrônicos, o próprio Poder Executivo percebeu a necessidade de criar normas que disciplinassem elaboração, o envio e o armazenamento de documentos eletrônicos em sua própria esfera de atuação.

O decreto nº 2.954, de 29 de Janeiro de 1999 estabeleceu regras para os atos normativos de competência do Poder Executivo e logo instituiu que a transmissão deveria ser feita em meio eletrônico, "exceto nos casos em que fosse impossível a utilização desse meio" (decreto 3.779/2001). Para assegurar a integridade e autoria dos documentos, o decreto de nº 3.714/2001 estabeleceu que os documentos deveriam ser assinados eletronicamente para a garantia da "segurança, autenticidade e integridade de seu conteúdo" e tramitados através de um sistema denominado SIDOF – Sistema de Geração e Tramitação de Documentos Oficiais (decreto nº 4.522/2002). Atualmente, toda essa tramitação é regida pelo decreto nº 4.176 de 28 de março de 2002.

No ano 2000, o Governo Brasileiro lançava as bases para a criação de uma sociedade digital ao criar um Grupo de Trabalho Interministerial com a finalidade de examinar e propor políticas, diretrizes e normas relacionadas com as novas formas eletrônicas de interação. As ações desse grupo de trabalho, foram ao encontro das metas do programa Sociedade da Informação, coordenado pelo Ministério da Ciência e Tecnologia. Esse esforço conjunto acabou por criar o que foi denominado de Governo Eletrônico [74], que tem como principais linhas de ação a promoção da universalização do acesso aos serviços, a transparência de suas ações, a integração de redes e o alto desempenho dos seus sistemas, todas essas ações em prol de um melhor atendimento aos anseios da sociedade.

Nesse ínterim, o governo cria a ICP-Gov (decreto nº 3.587/2000), ou seja, uma Infra-estrutura de Chaves Públicas que definia a organização, o modelo operacional e uma política de certificação através do uso de criptografia assimétrica para o Poder Executivo. Outros setores da sociedade, como a Caixa Econômica Federal, a SERASA, o SERPRO, incluindo o Poder Judiciário, já estavam em passos adiantados implementando suas próprias Autoridades Certificadoras.

Em 28 de junho de 2001, o Presidente da República edita a MP 2.200 e institui a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), com o objetivo de fazer com que órgãos governamentais e instituições privadas brasileiras pudessem usufruir de uma infra-estrutura capaz de suportar os fundamentos técnicos e legais de um sistema de certificação digital baseado em chave pública. Em razão de seu conteúdo, recebeu inicialmente várias críticas e foi re-editada por duas vezes. O próximo capítulo desse trabalho, irá analisar com mais detalhes as implicações técnicas e legais dessa MP e de outros projetos de lei.

Posteriormente, os decretos 3.865/2001, 3.996/2001 e 4.414/2002, estabeleceram regras sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Adicionalmente, o Comitê Gestor da ICP-Brasil aprovou em 18/04/2006 as Resoluções de nºs 38 a 45. Essas resoluções aprovam um conjunto de 8 documentos, que, juntamente com aqueles aprovados pela Resolução 15, de 10 de junho de 2002 e pela Resolução 36, de 21 de outubro de 2004, formam o corpo básico da Estrutura Normativa da ICP-Brasil. A criação e alteração dos documentos são sempre aprovadas pelo Comitê Gestor da ICP-Brasil, por meio de Resoluções [75].

A criação da ICP-Brasil e a possibilidade de atender os requisitos de integridade e autenticidade de um documento eletrônico através da certificação digital, têm impulsionado várias discussões sobre comércio eletrônico, o que parece ser uma das molas propulsoras na

definição de normas e projetos de lei. Criado pela Portaria Interministerial nº 42 de 2000 e tendo obtido inicialmente resultados incipientes, o Comitê Executivo de Comércio Eletrônico [76] foi reinstaurado em 2004. É essencialmente, uma interface entre os setores público e privado e visa melhor compreender e acelerar o desenvolvimento do comércio eletrônico no Brasil. Agora com o apoio total do Governo, o Comitê tem as seguintes prioridades: aprovação dos marcos legais faltantes, inclusão digital, definição de padrões e métricas da economia digital. O Comitê propõe ainda a discussão de temas como documento e fatura eletrônica, *spam*, simplificação burocrática e proteção de dados, entre outros [77].

A seguir será apresentada uma síntese dos principais decretos e medidas provisórias discutidas nessa seção, agrupados por afinidade, como também os projetos de lei que ainda estão em tramitação no Congresso Nacional. Também serão relacionadas as resoluções que dizem respeito ao funcionamento da ICP-Brasil aprovadas por seu Comitê Gestor.

<u>Decretos e Medidas Provisórias</u>

1) Decreto nº 4.176, de 28 de março de 2002 *(Vigente)*
Estabelece normas e diretrizes para a elaboração, a redação, a alteração, a consolidação e o encaminhamento ao Presidente da República de projetos de atos normativos de competência dos órgãos do Poder Executivo Federal, e dá outras providências. Em seu art. 37 estabelece que as propostas de projetos de ato normativo deverão ser encaminhadas à Casa Civil por meio eletrônico. No § 1º do Inciso III do mesmo artigo, normatiza que a exposição de motivos e o parecer jurídico conclusivo serão assinados eletronicamente.

> **Decreto nº 2.954, de 29 de Janeiro de 1999** (*Revogado pelo Decreto nº 4.176)*
> Estabeleceu regras para a redação de atos normativos de competência dos órgãos do Poder Executivo, pois considerava uma necessidade o controle de juridicidade e legitimidade dos atos normativos, assim como a uniformização dos atos e procedimentos administrativos.
>
> **Decreto nº 3.585, de 05 de setembro de 2000** (*Revogado pelo Decreto nº 4.176)*
> Incluiu o art. 57-A ao Decreto 2.954, acrescentando que a partir de 1º de janeiro de 2001, os documentos a que se refere este Decreto somente seriam recebidos, na Casa Civil da Presidência da República, por meio eletrônico.
>
> **Decreto nº 3.714, de 03 de Janeiro de 2001** (*Revogado pelo Decreto nº 4.176)*
> Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto no 2.954, de 29 de janeiro de 1999. Em seu artigo 2º expõe: "*A transmissão dos documentos a que se refere este Decreto, assinados eletronicamente pela autoridade competente, far-se-á por sistema que lhes garanta a segurança, a autenticidade e a integridade de seu conteúdo, bem como a irretratabilidade ou irrecusabilidade de sua autoria*".

Decreto nº 3.779, de 23 de Março de 2001 (*Revogado pelo Decreto nº 4.176)*
Acresce dispositivo ao art. 1º do Decreto no 3.714, de 3 de janeiro de 2001, que dispõe sobre a remessa por meio eletrônico de documentos.
"*Parágrafo único. Será utilizado o meio eletrônico, na forma estabelecida neste Decreto, para remessa de aviso ministerial, exceto nos casos em que for impossível a utilização desse meio.*"

2) Medida Provisória nº 2.200-2, de 24 de Agosto de 2001 *(Vigente)*

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil e transforma o Instituto Nacional de Tecnologia da Informação (ITI) em autarquia. A ICP-Brasil visa garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais. Foi primeiramente editada em 28 de Junho de 2001 (MP 2.200) e reeditada por duas vezes (MP 2.200-1 de 27 de julho de 2001 e MP nº 2.200-2, de 24 de agosto de 2001). Tem força de lei em razão da EC 32 de 2001, uma vez não foi revogada ou deliberada em definitivo pelo Congresso Nacional.

Decreto nº 3.872, de 18 de julho de 2001 *(Vigente)*
Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, seus integrantes e competências. Estabelece também que o CG receberá suporte técnico da Comissão Técnica Executiva – COTEC e assessoria do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações – CEPESC.

3) Decreto nº 3.996, de 31 de outubro de 2001 *(Vigente)*
Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Estabelece que somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital e os mesmos deverão ser providos mediante certificação disponibilizada por AC integrante da ICP-Brasil.

Decreto nº 4.414, de 07 de Outubro de 2002 *(Vigente)*
Altera o Decreto nº 3.996, acrescentando o art. 3º-A, que dispõe que "*As aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil.*"

Decreto nº 3.865, de 13 de Julho de 2001 *(Vigente)*
Estabelece requisito para contratação de serviços de certificação digital pelos órgãos públicos federais, e dá outras providências. Dispõe que somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos da Administração Pública Federal, direta e indireta, e as entidades a eles vinculadas poderão contratar, para uso próprio ou de terceiros, quaisquer serviços de certificação digital.

Decreto nº 3.587, de 05 de Setembro de 2000 *(Revogado pelo Decreto nº 3.996)*

Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov. Contemplou a organização, o modelo operacional e uma política de certificação através do uso de criptografia assimétrica. Um conjunto de regras e políticas ficaram de ser definidas por uma autoridade denominada de Autoridade de Gerência de Políticas – AGP.

4) Decreto nº 4.522, de 17 de Dezembro de 2002 *(Vigente)*
Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais – SIDOF, onde ficarão organizadas sob a forma de sistema, as atividades de elaboração, redação, alteração, controle, tramitação, administração e gerência das propostas de atos normativos a serem encaminhadas ao Presidente da República pelos Ministérios e órgãos integrantes da estrutura da Presidência da República.

<u>Resoluções do ITI</u>

Resolução n° 3, de 25 de Setembro de 2001 (*Vigente*)
Resolve designar Comissão para auditar a Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviços.

Resolução n° 5, de 22 de Novembro de 2001 (*Vigente*)
Aprova o Relatório de auditoria da AC Raiz.

Resolução n° 15, de 10 de Junho de 2002 (*Vigente*)
Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

Resolução n° 16, de 10 de Junho de 2002 (*Vigente*)
Estabelece as diretrizes para sincronização de freqüência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

Resolução n° 20, de 08 de Maio de 2002 (*Vigente*)
Determina o desenvolvimento de uma plataforma criptográfica aberta, voltada à operação da AC Raiz.

Resolução n° 29, de 29 de Janeiro de 2004 (*Vigente*)
Designa Comissão para realizar auditoria pré-operacional da AC Raiz em novo ambiente próprio devidamente provido de recursos físicos e lógicos.

Resolução n° 33, de 21 de Outubro de 2004 (*Vigente*)
Delega a AC RAIZ da ICP-Brasil atribuição para suplementar as normas do Comitê Gestor e dá outras providências.

Resolução n° 36, de 21 de Outubro de 2004 (*Vigente*)
Aprova o Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no âmbito da ICP-Brasil.

Resolução n° 38, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 da Declaração de Práticas de Certificação de Autoridade Certificadora Raiz da ICP-Brasil.

Resolução n° 39, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 da Política de Segurança da ICP-Brasil.

Resolução n° 40, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 dos Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil.

Resolução n° 41, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 dos Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil.

Resolução n° 42, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 dos Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.
Resolução n° 43, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 das Diretrizes da Política Tarifária da Autoridade Certificadora Raiz da ICP-Brasil.
Resolução n° 44, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 dos Critérios e Procedimentos para Realização de Auditorias nas Entidades nas Entidades da ICP-Brasil.
Resolução n° 45, de 18 de Abril de 2006 (*Vigente*)
Aprova a versão 2.0 dos Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP-Brasil.
Resolução n° 1, de 25 de Setembro de 2001 (*Revogada pela Res. 38 de 2006*)
Resolução n° 2, de 25 de Setembro de 2001 (*Revogada pela Res. 42 de 2006*)
Resolução n° 4, de 22 de Novembro de 2001 (*Revogada pela Res. 38 de 2006*)
Resolução n° 6, de 22 de Novembro de 2001 (*Revogada pela Res. 40 de 2006*)
Resolução n° 7, de 12 de Dezembro de 2001 (*Revogada pela Res. 41 de 2006*)
Resolução n° 8, de 12 de Dezembro de 2001 (*Revogada pela Res. 42 de 2006*)
Resolução n° 9, de 12 de Dezembro de 2001 (*Revogada pela Res. 42 de 2006*)
Resolução n° 10, de 14 de Fevereiro de 2002 (*Revogada pela Res. 43 de 2006*)
Resolução n° 11, de 14 de Fevereiro de 2002 (*Revogada pela Res. 41 de 2006*)
Resolução n° 12, de 14 de Fevereiro de 2002 (*Revogada pela Res. 40 de 2006*)
Resolução n° 13, de 26 de Abril de 2002 (*Revogada pela Res. 42 de 2006*)
Resolução n° 14, de 10 de Junho de 2002 (*Revogada pela Res. 40 de 2006*)
Resolução n° 17, de 20 de Setembro de 2002 (*Revogada pela Res. 40 de 2006*)
Resolução n° 18, de 10 de Outubro de 2002 (*Revogada pela Res. 43 de 2006*)
Resolução n° 19, de 08 de Maio de 2002 (*Revogada pela Res. 38 de 2006*)
Resolução n° 21, de 29 de Agosto de 2003 (*Revogada pela Res. 42 de 2006*)
Resolução n° 22, de 29 de Agosto de 2003 (*Revogada pela Res. 40 de 2006*)
Resolução n° 23, de 29 de Agosto de 2003 (*Revogada pela Res. 42 de 2006*)
Resolução n° 24, de 29 de Agosto de 2003 (*Revogada pela Res. 44 de 2006*)
Resolução n° 25, de 24 de Outubro de 2003 (*Revogada pela Res. 45 de 2006*)
Resolução n° 26, de 24 de Outubro de 2003 (*Revogada pela Res. 42 de 2006*)
Resolução n° 27, de 24 de Outubro de 2003 (*Revogada pela Res. 39 de 2006*)
Resolução n° 28, de 11 de Novembro de 2003 (*Revogada pela Res. 41 de 2006*)
Resolução n° 30, de 29 de Janeiro de 2004 (*Revogada pela Res. 42 de 2006*)
Resolução n° 31, de 29 de Janeiro de 2004 (*Revogada pela Res. 42 de 2006*)
Resolução n° 32, de 21 de Outubro de 2004 (*Revogada pela Res. 39 de 2006*)
Resolução n° 37, de 21 de Outubro de 2004 (*Revogada pela Res. 42 de 2006*)
Resolução n° 34, de 21 de Outubro de 2004 (*Revogada pela Res. 42 de 2006*)
Resolução n° 35, de 21 de Outubro de 2004 (*Revogada pela Res. 41 de 2006*)

Projetos de Lei

1) Projeto de lei nº 2.644, de 11 de dezembro de 1996

Autor: Dep. Jovair Arantes
Ementa: Dispõe sobre a elaboração, o arquivamento e o uso de documentos eletrônicos.
Apensado ao PL -1713/1996 – **Ementa:** Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências. Apensado

ao PL -1070/1995 – **Ementa:** Dispõe sobre crimes oriundos da divulgação de material pornográfico através de computadores.
Última Ação do PL -1070/1995: 14/12/2005 – Comissão de Constituição e Justiça e de Cidadania (CCJC). Designado Relator, Dep. Antonio Carlos Magalhães Neto.

2) Projeto de lei nº 3.173 de 26 de maio de 1997
Autor: Sen. Sebastião Rocha
Ementa: Dispõe sobre os documentos produzidos e os arquivados em meio eletrônico e dá outras providências.
Proposição Originária: PLS – 22/1996
Última Ação: 18/6/2001 – Mesa Diretora da Câmara dos Deputados. Recurso solicitando que este projeto seja apreciado pelo Plenário.

3) Projeto de lei nº 4.734 de 12 de agosto de 1998
Autor: Dep. Paulo Lima
Ementa: Dispõe sobre a informatização, no âmbito da Lei nº 6.015, de 31 de dezembro de 1973 - Lei de Registros Públicos - da escrituração cartorária através de discos ópticos e optomagnéticos ou em outros meios reconhecidos como legais, sem prejuízo dos métodos atualmente empregados. Incluindo o CD-ROM e o disquete.
Última Ação: 24/11/2000 - Encaminhado ao Senado Federal onde recebeu a designação de PLC 00109/2000 e desde a data de 12/06/2003 encontra-se na CCJC pronto para a pauta na comissão com voto pela aprovação do projeto.

4) Projeto de lei nº 1.532 de 19 de agosto de 1999
Autor: Dep. Angela Guadagnin
Ementa: Dispõe sobre a elaboração e arquivamento de documentos em meios eletromagnéticos.
Última Ação: 04/04/2006 – CCJC, para parecer com aprovação de mérito.

5) Projeto de lei nº 2.589 de 15 de março de 2000
Autor: Dep. Edison Andrino
Ementa: Altera o parágrafo único do artigo 541 do Código de Processo Civil - Lei nº 5.869, de 11 de janeiro de 1973, para admitir as decisões disponíveis em mídia eletrônica, inclusive na Internet, entre as suscetíveis de prova de divergência jurisprudencial, para os fins do artigo 105, III, c, da Constituição Federal.
Última Ação: 19/07/2006 – encaminhado à sanção presidencial.

6) Projeto de lei nº 4.906-A, de 21 de junho de 2001
Autor: Sen. Lúcio Alcântara com substitutivo do Dep. Júlio Semeguini
Proposição Originária: PLS-672/1999
Ementa: Dispõe sobre o comércio eletrônico. A este projeto estão apensados os PL 1.483/1999, 1.589/1999, PL 6.965/2002 e PL 7.093/2002.
Última Ação: 27/9/2001 – Mesa Diretora da Câmara dos Deputados, Leitura e publicação do parecer da Comissão Especial. Pronto para a Ordem do Dia.

> **Projeto de lei nº 1.483 de 12 de agosto de 1999**
> **Autor:** Dep. Hélio de Oliveira Santos
> **Ementa:** Institui a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico.
> **Última Ação**: 25/06/2001 – Apensado ao PL – 4.906/2001

Projeto de lei nº 1.589 de 31 de agosto de 1999
Autor: Dep. Luciano Pizzatto
Ementa: Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências.
Última Ação: 24/09/1999 – Apensado ao PL – 1.483/1999

Projeto de lei nº 6.965 de 12 de junho de 2002
Autor: Dep. José Carlos Coutinho
Ementa: Confere valor jurídico à digitalização de documentos, e dá outras providências.
Última Ação: 25/06/2002 – Apensado ao PL – 4.906/2001

Projeto de lei nº 7.093 de 6 de agosto de 2002
Autor: Dep. Ivan Paixão
Ementa: Esta lei dispõe sobre a correspondência eletrônica comercial, e dá outras providências.
Última Ação: 26/08/2002 – Apensado ao PL – 4.906/2001

7) Projeto de lei nº 7.316 de 07 de novembro de 2002
Autor: Poder Executivo
Ementa: Disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação. Define assinatura eletrônica avançada, chave de criação e de verificação de assinatura, certificado digital qualificado e outros. Estabelece requisitos para que a Autoridade Certificadora Raiz - AC Raiz da Infra-Estrutura de Chaves Públicas Brasileira realize o credenciamento de prestador de serviço de certificação.
Última Ação: 16/12/2005 – CCJC, parecer com complementação de voto, pela constitucionalidade, juridicidade, técnica legislativa e, no mérito, pela aprovação deste projeto, nos termos do Substitutivo da CCTCI (vide Anexo I), com subemendas; e das Emendas apresentadas nesta Comissão de nºs 1, com subemenda; 2, com subemenda; e 3 a 12.

Projeto de lei nº 6.825 de 17 de maio de 2002 *(Retirado e Arquivado)*
Autor: Poder Executivo
Proposição Originária: MSC-354/2002
Ementa: Cria a Taxa de Credenciamento de Autoridade Certificadora (AC), de Autoridade de Registro (AR) e dos demais prestadores de serviço de suporte à Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil e a Taxa de Fiscalização e de Manutenção de Credenciamento de atividades de certificação digital.
Última Ação: 20/10/2003 - Mesa Diretora da Câmara dos Deputados - Deferido o Aviso nº 1049/03, da Presidência da República, encaminhando a MSC 509/03, solicitando a retirada deste Projeto.Retirada deferida pela Mesa Diretora com base no inciso VII do Art. 114 do RICD.
OBS: PL retirado em razão da inadequação das taxas à realidade dos custos envolvidos na prestação de serviço de certificação, incluindo fiscalização, auditagem e credenciamento dos provedores de serviço de certificação.

Projeto de lei nº 2.281 de 10 de outubro de 2003 *(Retirado e Arquivado)*
Autor: Poder Executivo

Ementa: Institui a Taxa de Credenciamento - TCD, a Taxa de Fiscalização e de Manutenção de Credenciamento – TFM relativas às atividades de certificação digital, às multas e dá outras providências.
Última Ação: 27/04/2006 - Mesa Diretora da Câmara dos Deputados - Deferido o Aviso nº 385/06, da Presidência da República, encaminhando a MSC 268/06, solicitando a retirada deste Projeto.Retirada deferida pela Mesa Diretora com base no inciso VII do Art. 114 do RICD
OBS: PL retirado por inadequação à situação atual do ITI de recebimento de recursos do Tesouro Nacional e por estar em conflito com o PL 7.316.

8) Projeto de lei nº 229 de 22 de junho de 2005
Autor: Sen. Pedro Simon
Ementa: Dispõe sobre a autenticidade e o valor jurídico e probatório de documentos produzidos, emitidos ou recebidos por órgãos públicos federais, estaduais e municipais, por meio eletrônico.
Última Ação: 01/07/2005 – CCJC, aguardando designação do relator.

9) Projeto de lei nº 6.693 de 07 de março de 2006
Autor: Dep. Sandra Rosado
Ementa: Altera o art. 375 da Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil. Inclui o e-mail como prova documental, estabelecendo a presunção de autenticidade do mesmo.
Última Ação: 16/03/2006 – CCJC, sujeita à apreciação conclusiva pelas comissões.

Como pôde ser visto, o único instrumento com equivalência de lei que o Brasil possui relacionado a assinatura digital é a MP 2.200 (EC 32/2001). Todas as outras iniciativas relacionadas ao tema, ou são projetos de lei em tramitação ou decretos expedidos pelo Poder Executivo. Os decretos, deveriam somente elucidar e disciplinar a lei em seus aspectos empíricos. O que tem acontecido na prática é que muitos decretos são autônomos, tratam de assunto ainda não citado por lei, e assim acabam tendo a mesma força da lei no âmbito de sua aplicação.

O próximo capítulo procederá uma criteriosa análise crítica relacionada aos documentos eletrônicos e à assinatura digital. Essa análise apresentará questões de cunho técnico e também jurídico, inclusive analisando a legislação apresentada neste capítulo.

8. ANÁLISE CRÍTICA DE DOCUMENTOS ELETRÔNICOS E ASSINATURA DIGITAL

Esse capítulo apresenta uma análise técnica e legal dos diversos aspectos relacionados aos documentos eletrônicos e à certificação digital. A análise técnica procura mostrar que a segurança das assinaturas digitais vai além da criptografia e dos critérios exclusivamente técnicos, apresentando várias questões que podem ser discutidas em relação à segurança de um sistema de certificação digital. Já na seção seguinte são analisados os vários aspectos legais envolvidos, incluindo a legislação atual existente e as proposições em tramitação no Congresso Nacional.

8.1. ANÁLISE TÉCNICA

Com a popularização dos microcomputadores e o advento da Internet, a utilização de documentos eletrônicos vem crescendo constante e rapidamente. Esses documentos digitais têm como suporte o meio eletrônico, que oferece como vantagens a facilidade de processamento, a rapidez no trânsito de informações e a redução de custos. Novas características como a dissociabilidade do meio, a facilidade de alteração e duplicação, fizeram com que os conceitos de original e cópia se confundissem em um documento eletrônico digital.

A necessidade de garantir os requisitos de autenticidade, integridade e tempestividade de um documento eletrônico é importante para que o mesmo adquira validade e eficácia probatória e assim possa ser utilizado como meio de prova. A assinatura digital, proporcionada através da utilização da criptografia assimétrica, permite que tais requisitos sejam obtidos em conjunto com uma infra estrutura de certificação digital.

A utilização da criptografia é uma parte importante da certificação digital, provendo a segurança necessária para um documento eletrônico assinado digitalmente. Entretanto, deve-se observar que a criptografia é apenas uma parte de um sistema maior onde coexistem usuários, computadores, dispositivos de armazenamento, redes de comunicação, Autoridades Certificadoras e administradores desses recursos computacionais. Há uma máxima na segurança que afirma que "*a segurança de um sistema é tão forte quanto o seu elo mais fraco*". Por isso, a segurança fornecida pela criptografia é necessária, mas não suficiente,

para garantir os requisitos de segurança necessários ao funcionamento de uma infra-estrutura de certificação digital.

A seguir serão apresentadas diversas questões que podem dificultar o uso, ou até mesmo comprometer a confiança na utilização de um documento eletrônico contendo assinatura digital. Todas essas questões estão inter-relacionadas, mas para dar maior clareza ao texto, foram divididas em tópicos relacionados às pessoas (usuários e administradores), à infra-estrutura (equipamentos, normas e procedimentos) e aos softwares utilizados, de acordo com a ênfase que se quis dar ao tópico apresentado.

8.1.1. Questões relacionadas às pessoas

Esclarecimento dos conceitos de assinatura em meio eletrônico

É importante levar em consideração que a assinatura eletrônica é toda e qualquer forma de identificação efetuada por meio eletrônico. Uma senha digitada em uma página da internet é uma forma comum de exemplificar uma assinatura eletrônica. Já uma assinatura digital é um tipo de assinatura eletrônica, baseada na criptografia assimétrica e na utilização de certificados digitais. Percebe-se que esses dois conceitos, muitas vezes são utilizados como sinônimos, ou pior ainda, utiliza-se o conceito de assinatura digital de forma equivocada, às vezes referindo-se a uma assinatura digitalizada, que não tem qualquer amparo legal. É importante ressaltar que a assinatura digital pressupõe uma infra-estrutura de chaves públicas e a utilização de certificados digitais.

Uso correto da tecnologia e segurança do usuário

Os usuários de certificados e assinaturas digitais devem ter o conhecimento mínimo da tecnologia empregada e a consciência de que são parte integrante da “cadeia” de certificação necessária a dar credibilidade ao documento eletrônico assinado. Em especial, devem estar atentos a tentativas de “engenharia social”, a importância do sigilo da chave privada e a guarda dos dispositivos de armazenamento (normalmente um “*smart car*d” ou “*token*”). Nesse ínterim, é sabido que o conhecimento da chave privada do usuário por terceiros pode permitir a falsificação de assinaturas digitais de forma irrepudiável, caso a perda não seja imediatamente comunicada a Autoridade de Registro [78].

Os tipos de certificados mais utilizados e disponibilizados pelas Autoridades Certificadoras são os do tipo A1 e do tipo A3. Algumas ações podem danificar e inutilizar um certificado digital. Para os certificados do tipo A1, que são gerados e armazenados no

computador onde foi feita a solicitação, algumas considerações importantes devem ser observadas:

- O certificado A1, não usa "*smart card*" ou "*token*", devendo os dados nele contidos ser protegidos por uma senha de acesso. Somente com esta senha é possível acessar, mover e copiar a chave privada. O esquecimento da senha de acesso inutiliza o certificado, uma vez que não há meio de recuperá-la.
- O certificado do tipo A1 pode ser solicitado através da Internet. Após o processo de solicitação, o mesmo somente poderá ser instalado no mesmo computador onde foi solicitado, ou seja, no mesmo perfil de usuário e no mesmo navegador de Internet onde foi realizada a solicitação. A instalação em outro computador somente após a instalação inicial e posterior exportação do certificado.
- A formatação do computador ou a reinstalação do sistema operacional inutiliza o certificado digital, pois compromete a chave privada. Adicionalmente, qualquer alteração no perfil do usuário também pode comprometer a chave privada. A perda ou adulteração da chave privada, implica na perda do certificado digital pois a mesma não pode ser recuperada.

Para os certificados do tipo A3, as seguintes observações são muito importantes para o seu uso de forma correta e segura:

- O certificado do tipo A3 somente pode ser armazenado em "*smart card*" ou "*token*" criptográfico e a identificação do usuário deve ser obrigatoriamente presencial.
- Deve-se manter o "*smart card*" ou "*token*" em local seguro. Perdê-lo significa perder o certificado digital. A perda deve ser comunicada imediatamente a Autoridade de Registro para que se proceda a revogação do certificado.
- Danos físicos ao "*smart card*" ou "*token*" podem inutilizá-lo, tendo como conseqüência a perda do certificado.
- Esquecer as senhas do "*smart card*" e de acesso ao certificado também inviabiliza o seu uso, uma vez que não há meio de recuperá-las.
- Formatar o "*smart card*" ou "*token*" ou remover as chaves do dispositivo, também inutilizam o certificado.
- O dispositivo ("*smart card*" ou "*token*") pode ser bloqueado após a digitação sucessiva de senhas incorretas. É possível desbloqueá-lo, através de processo estabelecido com a Autoridade de Registro.

Adicionalmente, o computador utilizado pelo usuário para proceder à assinatura digital de um documento eletrônico deve possuir as condições mínimas de segurança para a realização de tal procedimento. É necessário manter o sistema operacional e o navegador de internet sempre em suas versões mais atuais, com atenção especial às atualizações de segurança. É muito importante a utilização de programas antivírus e "*firewall*" para proteção

de ataques vindos da rede de comunicação. Vírus e outros softwares mal intencionados, podem danificar e até mesmo apagar documentos de um computador desprotegido. No caso de certificados do tipo A1, que podem residir no disco rígido do computador, um vírus pode tentar "assinar" um documento não pretendido pelo usuário, daí a importância do uso de dispositivos mais seguros de armazenamento, a exemplo dos "*smart cards*" e "*tokens*" criptográficos. A utilização de senhas "fortes", que possuam ao menos letras e números, não relacionados ao usuário, é também um cuidado importante a ser observado.

Por fim, no caso de uso de certificados para sigilo (do tipo S1 a S4), o usuário deve guardar a sua chave privada mesmo após a expiração do correspondente certificado sob pena de não conseguir acessar os dados cifrados no futuro.

Qualificação técnica e capacitação

O esclarecimento mínimo das questões técnicas e conceitos que envolvem os serviços oferecidos por uma Infra-estrutura de Chaves Públicas é um requisito muito importante para que os usuários utilizem corretamente a tecnologia, e assim, possam usufruir de seus benefícios. Tão importante quanto o esclarecimento dos usuários, é o treinamento e a qualificação técnica dos empregados e prestadores de serviço das entidades que compõem uma hierarquia de certificação.

Hoje a grande maioria da população desconhece o que é a certificação digital e as suas implicações práticas. Mesmo entre os técnicos, há poucas pessoas que dominam o assunto; e dentre essas pessoas há diferentes níveis de conhecimento, dada a complexidade que envolve todo o aparato técnico de uma ICP. O investimento em capacitação técnica permitirá que os setores da sociedade que estão há mais tempo fazendo uso dessa tecnologia, como por exemplo o setor financeiro e alguns órgãos públicos, possam viabilizar novas aplicações e enfrentar os desafios que ainda existem para promover o uso da certificação digital no Brasil.

O surgimento de novas aplicações e serviços que utilizem os certificados digitais, aliado ao investimento em capacitação técnica, podem dar um novo impulso à popularização dos certificados digitais. A qualificação em tecnologia da informação de uma forma geral, permite diminuir a exclusão digital, na medida em que pode ser uma forma de melhorar a condição de vida da população brasileira, ajudando a superar um "*apartheid*" digital existente em vários setores da sociedade.

8.1.2. Questões relacionadas à infra-estrutura

Utilização de uma infra-estrutura e confiança nas chaves públicas

Para certificar-se que um documento eletrônico contém uma assinatura digital válida, faz-se necessária a utilização da chave pública. Entretanto, caso esse documento seja enviado para outra pessoa juntamente com a chave pública para verificação, não mais é possível ter a garantia da integridade do documento em questão. Se um terceiro interceptar o documento e a chave pública durante o envio, é possível a alteração do documento original e a geração de uma nova chave pública a partir de uma chave pública qualquer. O destinatário final, utilizando-se da chave pública enviada, acreditará tratar-se do documento original. Esse tipo de ataque é denominado "*man in the middle*" [79].

A certificação digital surgiu para evitar esse tipo de situação. A Autoridade Certificadora possui registrada a chave pública do emissor do documento, podendo identificar como original, o documento inicialmente assinado. Dessa forma, basta ao destinatário conhecer a chave pública da Autoridade Certificadora, que possui notoriedade e publicidade, pois é utilizada para todas as assinaturas digitais emitidas pela mesma. A confiança no documento eletrônico, nesse caso, resume-se na confiança e idoneidade da Autoridade Certificadora: tendo confiança na Autoridade Certificadora, automaticamente confia-se no documento eletrônico certificado por essa entidade.

Interoperabilidade de software e hardware

Por interoperabilidade pode-se entender a capacidade dos equipamentos e dos programas utilizados em uma infra-estrutura, como por exemplo a ICP-Brasil, de comunicarem-se entre si independente de sua procedência ou fabricante. Em um panorama ideal para uma infra estrutura de chaves públicas, a interoperabilidade seria a possibilidade de um usuário utilizar seu certificado digital para criar e verificar as assinaturas digitais, independente do fornecedor do programa ou do equipamento utilizado.

Hoje, isso é um grande desafio. Apesar da existência de normas como a ISO 7816 e o padrão PKCS ("*Public-Key Cryptography Standards*"), grande parte dos leitores de "*smart cards*" não são intercambiáveis entre si e os "*tokens*" também não possuem drivers compatíveis. Em muitas situações, um determinado cartão "*smart card*" não conseguirá ser lido por uma leitora de outro fabricante. Para que a certificação digital possa atingir o crescimento desejado, ou seja, o serviço fornecido tiver por escopo a coletividade, é

fundamental que haja um esforço de padronização dos instrumentos de software ou hardware. Assim, evita-se que as aplicações desenvolvidas e os serviços fornecidos aos usuários não fiquem com abrangência limitada, o que afetaria diretamente a escalabilidade de uma infra-estrutura de chaves públicas.

A Resolução nº 36 de 21/10/2004, emitida pelo Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira, regulamentou o processo de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil. Coube ao ITI, enquanto Autoridade Certificadora Raiz, a responsabilidade da condução dessa atividade. Nesse ínterim, a ICP-Brasil apresenta um razoável esforço para alcançar a interoperabilidade entre soluções de diversos fornecedores em um único domínio, mas ainda é necessário que a mesma esteja preparada para estabelecer um modelo de atuação com outros domínios de ICP, sejam eles nacionais ou internacionais [80]. Parafraseando Peter Alterman [81]: "*PKI* [6] *is no good if you are only talking to yourself*", resume a importância da padronização e interoperabilidade entre os dispositivos e aplicações envolvidos em uma infra-estrutura de chaves públicas como a ICP-Brasil. Por fim, a padronização e a interoperabilidade podem ser importantes elementos na redução dos custos dos dispositivos de armazenamento utilizados pelos usuários da certificação digital.

Auditoria

Apesar da existência da MP 2.200-2 que garante a validade jurídica de um documento eletrônico certificado pela ICP-Brasil, uma das grandes forças que impulsionará o uso da certificação digital é a confiança nas entidades participantes por parte do usuário final. Não haverá lei que fará um usuário ter confiança nas Autoridades Certificadoras (ACs), em especial na AC-Raiz. O usuário deve confiar no processo de obtenção do seu certificado digital, na idoneidade dos softwares utilizados para criar e verificar as assinaturas digitais, nos dispositivos de armazenamento de sua chave privada, enfim, em todas as etapas necessárias à obtenção e utilização de seu certificado digital. Essa confiança não pode ser imposta, tem que ser adquirida. Uma das formas de obter essa confiança é a possibilidade da realização de auditorias externas com o objetivo de garantir transparência aos processos envolvidos.

Uma auditoria deve envolver avaliações independentes das políticas da organização, da segurança dos seus ambientes físico e lógico, dos procedimentos, dos padrões

---

[6] PKI é um acrônimo em inglês de Private Key Infrastructure, equivalente a ICP em português.

e das práticas para salvaguarda das informações eletrônicas evitando a perda, o dano, a indisponibilidade da informação e a revelação de informações sigilosas.

A auditabilidade e fiscalização dos softwares utilizados na ICP-Brasil hoje é parcial e realizada pelo próprio Comitê Gestor da ICP-Brasil (MP 2.200-2 art. 4º, Inc. IV). A plataforma utilizada para os serviços de certificação é proprietária e possui patentes, que os fornecedores tem chamado de “segredos de negócio”, o que impede uma auditoria em seus códigos fonte. Porém, como já foi citado anteriormente, o Brasil tem a intenção de nacionalizar a plataforma de software e hardware utilizados na ICP-Brasil através do “Projeto João-de-Barro” o que viabilizaria uma auditoria externa plena.

Segurança física e lógica da infra-estrutura

Atualmente, no momento em que o conhecimento e a informação são fatores de suma importância para qualquer organização, a segurança da informação é um pré-requisito indispensável para todo e qualquer sistema de informações, principalmente para uma Infra-estrutura de Chaves Públicas (ICP). Uma ICP está a merce dos mais variados tipos de ameaças, como fraudes, interrupção dos serviços, revelação de informações sigilosas, acessos não autorizados, sabotagens, dentre outros. Para tratar essas ameaças, torna-se necessário a definição de políticas e mecanismos de segurança, visando dar suporte à prevenção, detecção e contingência de qualquer tipo de incidente. Com isso, é possível estar preparado para evitar fraudes, detectar tentativas de comprometimento da segurança e até mesmo interromper um ataque ao sistema. A detecção e a interrupção de um ataque deve acionar um plano de contingência, com o objetivo de avaliar e reparar danos, além de manter a operacionalidade dos serviços disponíveis aos usuários.

A segurança física inclui um ambiente físico apropriado como uma sala cofre para abrigar os computadores e equipamentos de rede como “*switches*”, roteadores e dispositivos de armazenamento de dados. A segurança física também inclui a proteção da infra-estrutura das redes de telecomunicação e energia, prevendo riscos como incêndios, inundações e manifestações.

A segurança lógica é tão importante quanto a segurança física do ambiente. A segurança lógica inclui o controle de acesso e proteção dos recursos computacionais, uso de “*firewalls*” e IDS (“*Intrusion Detection Systems*”), gerenciamento de vulnerabilidades, registros de “*logs*”, proteção de dados sigilosos, política de “backup”, plano de recuperação de desastres, auditoria e segurança dos equipamentos e programas utilizados.

8.1.3. Questões relacionadas aos softwares utilizados

Utilização de algoritmos comprovadamente seguros

Alguns algoritmos de criptografia assimétrica são sabidamente inseguros e isso já foi comprovado com ataques práticos. Como exemplo podemos citar o algoritmo de Merkle-Hellman [82] baseado no problema de Knapsack, que foi quebrado por Adi Shamir [83], alguns anos após a sua criação. Entretanto, os algoritmos mais utilizados atualmente, o DSA e o RSA são considerados computacionalmente seguros. O NIST tem constantemente revisado o padrão DSS (*Digital Signature Standard*) e espera-se em breve o anúncio do FIPS 186-3, que possibilitará a utilização dos algoritmos de "*hashing*" SHA2 (SHA-256, SHA-384, SHA-512) com o algoritmo DSA. Uma variação de utilização do DSA utiliza curvas elípticas (ECDSA), o que possibilitaria o uso de chaves de menor tamanho, com o mesmo nível de segurança. Porém, a utilização de curvas elípticas para algoritmos assimétricos é um assunto relativamente recente, embora já esteja em andamento sua aprovação para uso com o padrão DSS [84].

Em relação a criptografia simétrica a recomendação é a utilização do AES (*Advanced Encryption Standard*) – Rijndael, com tamanho de chave de pelo menos 128 bits. Em razão de ataques conhecidos como "*birthday attack*" e "*meet in the middle*", SCHNEIER e FERGUSON [29], sendo um pouco conservadores ao tratar do assunto, recomendam como uma regra de projeto que "*para um nível de segurança de n bits, considere a utilização de pelo menos 2n bits*". Assim, é recomendada a utilização de 256 bits como tamanho de chave para qualquer algoritmo de cifragem com requisito de 128 bits. Adicionalmente, todos os finalistas do concurso para escolha do AES, são algoritmos considerados muito seguros, em particular o algoritmo Serpent, considerado o "mais seguro" em razão do seu caráter conservador. Não foi escolhido como AES em razão de ter sido considerado lento (equivalente em velocidade ao DES) e não tão flexível quanto o algoritmo Rijndael (AES) [29].

Ainda em relação à segurança dos algoritmos, a geração de chaves é muito importante para a segurança das funções criptográficas. A mesma pressupõe a utilização de um gerador de números randômicos. A dificuldade de obtenção de dados randômicos reais, faz com que na prática, sejam utilizados números pseudo-randômicos, computacionalmente seguros e gerados a partir de dados randômicos. É importante observar, que os números pseudo-randômicos não podem ser previsíveis e devem possuir o máximo de entropia, sob pena de comprometimento da segurança. É clássico o exemplo da quebra da criptografia do

navegador Netscape em sua versão 1.1 [30], onde uma chave de 128 bits na verdade continha cerca de 20 bits de entropia, o que tornava a segurança do algoritmo não melhor do que uma chave de 2^{20}.

Algoritmos utilizados na ICP-Brasil

Os documentos de REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-05) e PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC-ICP-01.01), ambos vinculados à resolução nº 42 de 2006 da legislação da ICP-Brasil, estabelecem a utilização do algoritmo RSA de 2048 bits para geração de chaves assimétricas de uma AC; para o usuário final o tamanho varia de 1024 à 2048 bits de acordo com o tipo de certificado utilizado (de 1 a 3 – 1024 bits, 4 – 2048 bits), conforme já apresentado na Tabela 6.1 no capítulo 6 deste trabalho. A função de "*hashing*", de acordo com as normas, seria a implementação do SHA-1. A utilização desses algoritmos e chaves pode ser considerada adequada em razão dos algoritmos SHA-2 ainda não terem sido lançados como padrão pelo FIPS. Os algoritmos utilizados pela ICP-Brasil devem ser periodicamente atualizados, em razão da evolução constante da tecnologia. Em particular, a criação de eficientes algoritmos de fatoração e o surgimento de novas técnicas de criptoanálise não podem ser menosprezados [31].

Com relação aos algoritmos simétricos utilizados para cifragem da chave privada da entidade titular e de seu "*backup*", as resoluções da ICP recomendam a utilização do 3DES (168 bits), do IDEA e do SAFER+, esses dois últimos com 128 bits. Deixando o preciosismo de lado, em razão do AES estar disponível há mais de 5 anos, o mesmo poderia ter sido indicado ao menos como opção de algoritmo criptográfico simétrico a ser utilizado no âmbito da ICP-Brasil.

Justifica-se: 1) O 3DES, em razão do ataque "*meet in the middle*" possui uma efetiva segurança equivalente a 112 bits em vez dos 168 bits que compõe as suas 3 chaves [85]. Em razão de seu projeto, o DES, e em conseqüência o 3DES, não tem boa performance na implementação através de software. O AES tende a ser cerca de 6 vezes mais rápido, além de ter uma margem de segurança bem maior: tamanho de bloco maior (128 bits x 64 bits do DES), possibilidade de uso de chaves de 128, 192 e 256 bits, sendo resistente à criptoanálise. 2) O IDEA (*International Data Encryption Algorithm*) concebido no início dos anos 90 usa também um bloco de 64 bits e, até o ano de 2004, o melhor ataque conhecido para qualquer chave conseguiu quebrar 5 rodadas ("*rounds*") de um total de 8,5 [86]. SCHNEIER, já em

1999, não mais recomendava o seu uso em razão da disponibilidade de algoritmos mais rápidos, progressos na área de criptoanálise e também pela existência de patentes do algoritmo IDEA até o ano de 2011 [86]. 3) O SAFER+, de 1998, tem bloco de 128 bits e é baseado no algoritmo SAFER K-64 (*Secure And Fast Encryption Routine*) originalmente proposto em 1993. Foi submetido para o concurso de escolha do AES e não foi escolhido entre os finalistas [87]. Então por que não optar pelo AES, que inclusive é disponível sem custos para utilização em qualquer propósito ? Fica a questão.

Em 2004, foi lançado no Brasil um projeto denominado "Projeto João-de-Barro", com o objetivo de criar um módulo criptográfico (software e hardware) para a emissão das chaves públicas e privadas das Autoridades Certificadoras integrantes da ICP-Brasil. A idéia é nacionalizar a plataforma, desenvolvendo tecnologia própria através da utilização de software livre. Além do ITI, participam do projeto diversas entidades, entre elas a UFSC (Universidade Federal de Santa Catarina), o ITA (Instituto Tecnológico da Aeronáutica) e o CASNAV (Centro de Análises de Sistemas Navais). No 4º CertForum [88], realizado entre 8 e 10 de agosto de 2006 em Brasília, foi apresentado o software de gerenciamento de certificado digitais desenvolvido pela UFSC. A partir de setembro, começa a integração com o hardware que está sendo desenvolvido pelo ITA.

Atualmente, a plataforma que produz e viabiliza toda a cadeia de certificação brasileira pertence a uma empresa multinacional, com software proprietário o que inviabiliza sua auditoria plena.

Qualidade do software

A implementação de um algoritmo comprovadamente seguro não deve possuir erros ou falhas que possam dar a chance de algum tipo de ataque ou comprometimento da segurança do software utilizado. De nada adianta a utilização de um algoritmo comprovadamente seguro em uma implementação fraca e com erros de programação. No caso das assinaturas digitais, não se pode esquecer de que é necessário um software que realize os procedimentos necessários para efetivar a assinatura em um documento eletrônico. A comprovação da qualidade do software e aderência à especificação dos algoritmos implementados é uma tarefa difícil de ser comprovada, uma vez que a maioria deles é proprietário e muitas vezes protegidos por patentes.

Nesse sentido, cabe ressaltar a importância do ITI ter colocado à disposição da sociedade, sob a licença GPL/GNU [7], três aplicativos desenvolvidos por meio de licitação pública, conforme publicado no Diário Oficial da União do dia 28/06/2005, na forma da Portaria nº 41. A Certisign desenvolveu o Assinador Digital e coube à Módulo Security a responsabilidade sobre o Módulo PAM e o Chaveiro Digital [89]. A possibilidade de ter acesso ao código fonte desses aplicativos é muito importante, pois permite que empresas e usuários possam contribuir para melhoria do software, em especial nas questões relacionadas à segurança e qualidade das aplicações disponibilizadas. A seguir são apresentadas as principais características dos programas disponibilizados.

O PAM ("*Pluggable Authentication Module*") permite a utilização de um certificado digital na autenticação de usuários em uma rede de computadores, em substituição ao tradicional par de usuário e senha. O Chaveiro Digital realiza a tarefa de assinatura e cifragem de mensagens enviadas por meio de correio eletrônico, além de possibilitar o acesso às funcionalidades dos navegadores de Internet na requisição de serviços com certificação, suportando "*smart cards*" e "*tokens*". Por fim, o Assinador Digital é uma interface gráfica padrão KDE que permite a assinatura e encriptação de qualquer arquivo digital. A aplicação possibilita, ainda, a execução de tarefas comuns relacionadas à certificação digital, como a gestão de chaves e listas de certificados revogados, permitindo inclusive o uso de certificados cujas chaves estejam armazenadas em "*smart cards*" ou "*tokens*".

Aqui cabe uma crítica construtiva em relação à disponibilização dos aplicativos acima citados. Segundo pesquisa da Fundação Getúlio Vargas [90], em abril de 2006, o Brasil possuía 32 milhões de computadores desktop, e destes, 97% utilizavam o sistema operacional Windows da Microsoft.

Já que um dos objetivos do ITI é disseminar a cultura e a utilização da certificação digital, é difícil entender por que motivo também não foram disponibilizados os programas para a plataforma Windows, que o ITI generaliza denominando-os de "plataforma proprietária", e afirma já ter portado as bibliotecas utilizadas no desenvolvimento das aplicações acima citadas.

Programas e tipos de documentos assinados

---

[7] GPL é uma Licença Pública Geral que dá liberdade de distribuir e alterar um sofware, garantindo que o mesmo será livre e gratuito para os seus usuários.

Muito se tem falado a respeito da utilização de assinaturas digitais e a garantia de autenticidade e integridade que as mesmas fornecem a um documento eletrônico digital. Qualquer tipo de documento ou arquivo pode ser efetivamente assinado, uma vez que em última análise todos são compostos por um conjunto de bits 0 ou 1. Se o arquivo for assinado por um certificado emitido pela ICP-Brasil, terá então a garantia de sua autenticidade, integridade e validade jurídica de acordo com as disposições da MP 2.200-2. Entretanto, um documento eletrônico precisa de um computador e de um programa para ser visualizado. É a partir dessa visualização que o usuário irá, a partir da sua chave privada, aplicar a sua assinatura digital com a utilização de um software apropriado. Essa situação faz com que exista a possibilidade de um usuário estar assinando algo diferente daquilo que ele vê representado na tela do computador, uma vez que a assinatura é realizada sobre um conjunto de bits e não sobre o resultado efetivamente visualizado pelo usuário. Para que isso aconteça na prática, é necessário que o programa utilizado para visualizar o documento seja modificado, de modo que a visualização seja diferente dos bits que estão efetivamente armazenados.

Isso pode parecer utópico e difícil de acontecer. Porém, deve-se lembrar que hoje utilizamos complexos programas de editoração de textos, como por exemplo o Word da Microsoft e o Writer do OpenOffice. Ambos possuem linguagens de macro incorporadas e capacidade de criação de campos calculados que podem buscar dados fora do documento original, inclusive de qualquer lugar na internet. Então vamos imaginar a situação em que o nome do usuário ou a data escrita em um documento seja um campo calculado. O usuário estará assinando aquilo que ele vê na tela, mas isso pode não representar aquilo que está gravado efetivamente no conjunto de bits assinado. Um campo calculado pode aceitar uma infinidade de fórmulas: pode-se fazer com que o nome de uma pessoa seja alterado a partir de determinada data; ou também, incrementar uma data futura representada no momento da assinatura, de modo que a mesma nunca seja alcançada. O que deve ficar claro aqui é que o campo calculado conforme representado no documento nunca seria alterado; o que muda é somente a sua visualização, ou seja, aquilo que é apresentado para usuário. Isso permite que um documento possa ser exibido de diversas formas, sem que a sua assinatura digital seja invalidada. Essas alterações na exibição de um documento podem ser detectadas por meio de uma perícia, mas mesmo nesse caso, talvez não seja mais possível obter o conteúdo original do documento no momento de sua assinatura.

Outra situação que pode invalidar uma assinatura é a alteração de metadados existentes nos documentos assinados. Metadados são informações adicionais sobre um documento, incorporadas automaticamente pelo editor de textos utilizado. Exemplos de metadados são o nome do usuário que criou o documento, a data de sua última modificação, a data de sua última impressão, o nome da empresa para qual o programa está registrado, etc. Uma simples impressão de um documento assinado digitalmente pode alterar o metadado que contém a data da última impressão; com a modificação do conteúdo do documento assinado a assinatura digital é automaticamente invalidada.

Essa questão não é um problema das assinaturas digitais em si, muito menos do modelo de infra estrutura de chaves adotado (seja a ICP-Brasil ou qualquer outra). É simplesmente decorrente das várias maneiras que um documento eletrônico pode ser apresentado e dos diversos programas que podem ser utilizados para a sua visualização. Com certeza, essa é uma questão muito importante para a popularização das assinaturas digitais. O tipo de documento a ser assinado, a confiança nos diversos programas utilizados – tanto para sua criação como para aposição de uma assinatura digital – ainda deverão ser amplamente discutidos até que a certificação digital tenha ampla aceitação e utilização pela sociedade.

A LCR e o risco dos certificados auto-assinados

As listas de certificados revogados (LCRs) são parte necessária e imprescindível à operação adequada de qualquer infra estrutura de chaves públicas. O comprometimento da chave privada, erros na emissão ou gerenciamento das chaves são exemplos de situações reais onde o certificado deve ser revogado. A possibilidade de ocorrência da revogação faz com que a verificação de sua validade seja um passo obrigatório para que um certificado revogado não seja aceito como válido. Garantir que a LCR esteja correta e atualizada é muito importante. Para a LCR ser efetiva, precisa estar sempre disponível (na Internet, por exemplo) e os programas utilizados para verificação dos certificados devem sempre utilizá-la, o que nem sempre acontece.

Uma alternativa ao uso das listas de certificados revogados é a utilização do protocolo OCSP (“*Online Certificate Status Protocol*”), que permite a verificação “*on-line*” da validade de um certificado evitando assim a necessidade de se obter sempre a LCR atual, que pode ser relativamente grande. A utilização do OCSP traz outras vantagens, como a tempestividade e a redução de custos, já que não se tem o ônus relacionado à atualização, gerenciamento e distribuição freqüente da LCR. Além disso, o uso de um protocolo de

consulta evita a exposição desnecessária do nome de todos os usuários com certificado revogado.

Outra questão diz respeito aos certificados auto-assinados. Eles são importantes pois finalizam a cadeia de certificação e são considerados íntegros, inclusive podendo assinar outros certificados. O certificado da ICP-Raiz é um certificado auto-assinado. Entretanto, qualquer pessoa, a partir de um software de ICP (existem versões gratuitas), tem a possibilidade de gerar certificados auto-assinados com qualquer informação desejada. O usuário ao receber um certificado auto-assinado receberá um alerta de que o certificado é de uma AC não confiável, embora tenha a opção de instalá-lo, "habilitando a confiança" em qualquer certificado emitido por esta AC.

Supondo que o usuário irá utilizar o certificado a partir de um navegador Internet (o Internet Explorer, por exemplo), o problema reside na possibilidade de um certificado auto-assinado de uma AC ser instalado externamente ao navegador, sem o conhecimento do usuário [91]. Essa possibilidade existe uma vez que o certificado pode residir com uma chave no registro do Windows ou um arquivo no sistema de arquivos. Dessa forma, um software mal intencionado, do tipo cavalo de tróia [92], pode instalar o certificado sem o consentimento e conhecimento do usuário. A partir desse ponto, qualquer certificado emitido por essa "falsa" Autoridade Certificadora, aparecerá para o usuário como um certificado emitido por uma autoridade confiável. Dessa constatação, recomenda-se que o usuário sempre confirme a legitimidade dos certificados instalados em seu computador e adote as medidas mínimas de proteção para o seu sistema operacional como a utilização de antivírus, "*antispyware*" e "*firewall*" [92], mantendo-os sempre atualizados.

8.1.4. Considerações

Uma infra-estrutura de certificação digital possui diversos aspectos técnicos com variados graus de complexidade. Nesse contexto, estão envolvidas pessoas, programas sofisticados e a própria estrutura necessária para o funcionamento dessa tecnologia. O usuário comum, apesar de ter responsabilidades (a guarda e o sigilo de sua chave privada talvez seja a principal delas), tem muito pouco controle em relação a complexidade que envolve uma ICP. Ele deve confiar em quem emitiu o seu certificado digital e se respaldar na responsabilidade das ACs e ARs em responder civilmente pelos danos causados em razão de erros ou fraudes na prestação do serviço de certificação digital. Como por exemplo, podemos citar aqueles decorrentes de uma identificação falsa ou de eventual revogação retroativa de um certificado.

A seguir, será apresentado um exemplo prático de como poderia acontecer um processo de contratação eletrônica, comparando-o com uma situação tradicional.

8.1.5. Exemplo Prático

Este item irá mostrar um exemplo prático de como poderia funcionar um processo ou fluxo de contratação eletrônica (Figura 8.2). Parte-se da premissa que ambos os contratantes já possuem os seus respectivos certificados digitais e as chaves privadas armazenadas em dispositivos do tipo "*smart card*". Será realizada uma breve comparação com um contrato tradicional da forma como é realizado hoje com o reconhecimento de firma e da assinatura em um cartório tradicional (Figura 8.1).

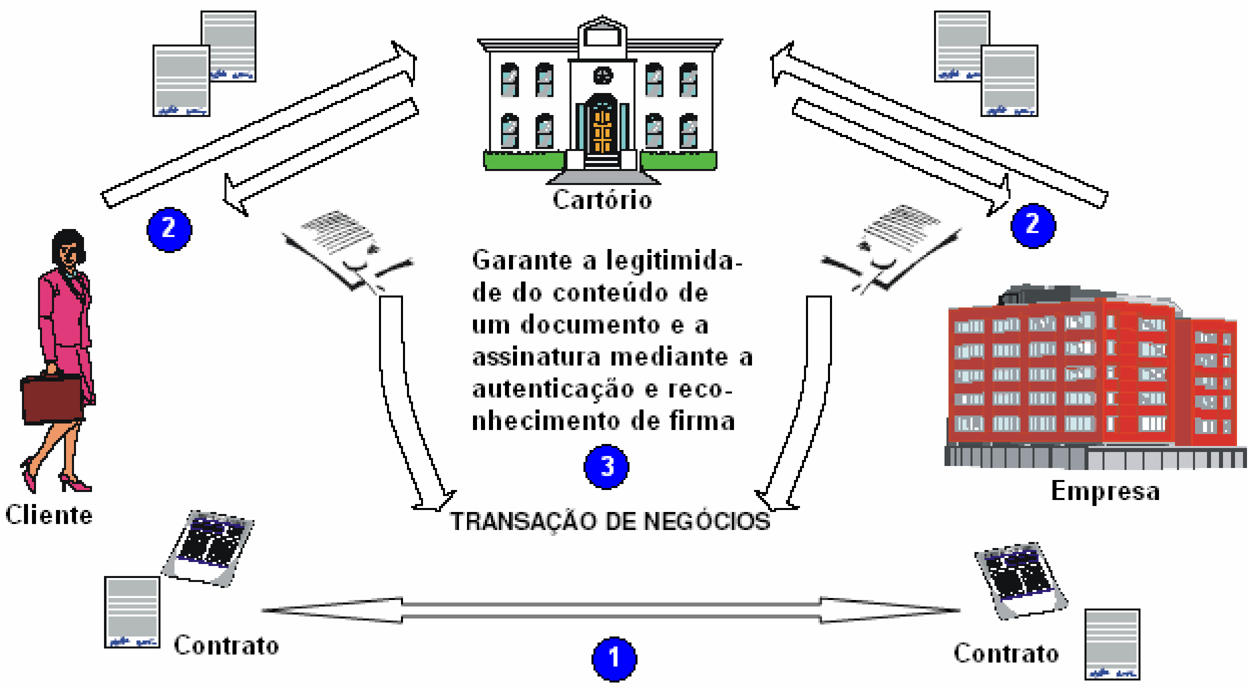


Figura 8.1 – Fluxo de contratação através de um documento tradicional

Na assinatura de um contrato tradicional, as cláusulas são discutidas entre as partes, conforme indica o passo 1 da Figura 8.1. Após acertadas as cláusulas do contrato, o contratante, nesse exemplo denominado de cliente e a contratada (empresa), devem se dirigir a um cartório a fim assinarem de próprio punho o contrato e após proceder o reconhecimento das respectivas firmas (assinaturas), garantindo assim a autenticidade e legitimidade do conteúdo do contrato (passos 2 e 3 da Figura 8.1).

Em uma contratação eletrônica, também denominando os contratantes de cliente e empresa, conforme exposto anteriormente, os seguintes passos são realizados (Figura 8.2):

1. As cláusulas do contrato são acertadas semelhante a contratação tradicional, com a facilidade da troca eletrônica de arquivos e mensagens;
2. A empresa, para proceder a assinatura digital do contrato, utiliza-se de um software para cifrar o "resumo" (*hash*) do documento com sua chave privada. Submete esse "resumo" a uma Autoridade de Carimbo de Tempo (TSA – *Time Stamping Authority*) que irá devolver o "resumo" assinado e protocolado com o horário da assinatura.
3. De posse desse "protocolo" o software de assinatura termina o processo de assinatura digital do contrato e o envia para o cliente.
4. O cliente confere, em uma Autoridade Certificadora (AC), se o certificado não foi revogado (verificando a LCR) e a idoneidade da chave pública correspondente a chave privada usada na assinatura feita pela empresa.
5. O cliente também entra em contato com uma Autoridade de Carimbo de Tempo (TSA) e recebe o correspondente protocolo, de forma idêntica ao item 2 realizado pela empresa.
6. De posse do protocolo, o cliente também termina o processo de assinatura digital iniciado com seu software e sua chave privada.
7. O contrato agora possui duas assinaturas digitais válidas e a empresa também pode conferir a assinatura do cliente e a LCR através da Autoridade Certificadora. O contrato também pode ser verificado, assinado digitalmente por um tabelião e armazenado em um repositório, aqui denominado de cartório virtual.

A grande vantagem do contrato assinado digitalmente é a não necessidade dos contratantes de se encontrarem fisicamente e comparecerem a um cartório tradicional, uma vez que todo o processo pode ser realizado pela Internet. Essa característica é especialmente útil para a utilização no comércio eletrônico realizado em uma loja virtual na Internet, por exemplo. Garante a identidade dos participantes (comprador e vendedor), a integridade do contrato e a tempestividade – requisitos esses indispensáveis à obtenção da validade jurídica de uma contratação virtual.

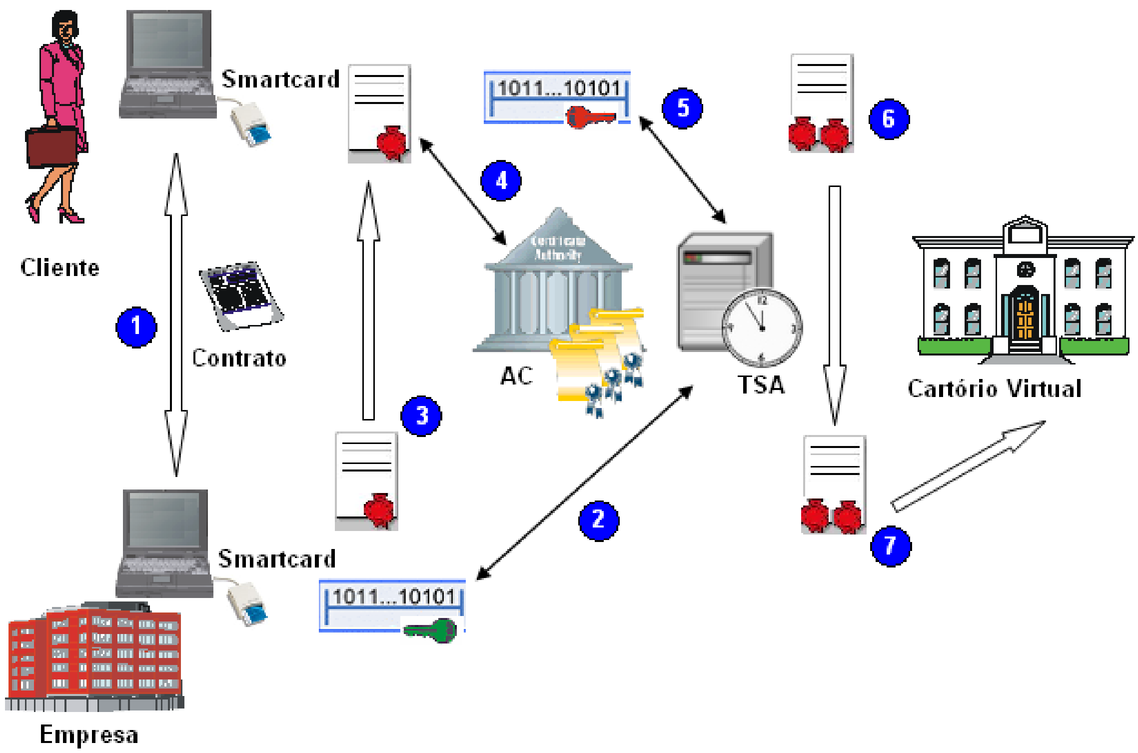


Figura 8.2 – Fluxo de contratação através de um documento com assinatura digital

8.2. ANÁLISE LEGAL

No item anterior, foram analisados diversos aspectos técnicos relacionados à utilização de documentos eletrônicos de forma idônea e segura. Com os princípios estabelecidos pela criptografia assimétrica, foi possível obter um método de garantir a integridade e a autenticidade de tais documentos ou mensagens em formato digital, desde que tomadas as devidas precauções em relação ao uso correto da tecnologia, sem desconsiderar os vários elementos coexistentes em uma infra-estrutura de certificação digital.

Como em qualquer situação de vanguarda tecnológica, a utilização de assinaturas digitais embora tecnicamente viável, no Brasil ainda carece de uma base legal sólida. Embora as assinaturas eletrônicas já estejam sendo utilizadas na prática, a legislação relacionada ao tema ainda não conseguiu acompanhar o mesmo ritmo da evolução tecnológica.

Nesta seção, será analisada a validade jurídica dos documentos eletrônicos, em especial aqueles assinados eletronicamente através do uso de assinaturas digitais e certificação digital. Também será realizada uma análise crítica da legislação atual existente no Brasil, incluindo Medidas Provisórias, Projetos de Lei em tramitação e questões relevantes que não foram mencionadas nas proposições. As principais proposições citadas no Capítulo 7 serão

comentadas e analisadas de forma que ao final dessa seção será possível compreender por que motivo muitas delas acabam sequer sendo apreciadas, inviabilizando totalmente a sua aprovação ou até mesmo rejeição perante o Processo Legislativo. Em especial, a discussão terá uma ênfase maior nos PL 1.589 (pelo seu caráter técnico e jurídico), nas várias versões da MP 2.200 e no PL 7.316, uma vez que este último tem a intenção de substituir a MP 2.200-2. O mesmo já possui parecer favorável na CCJC na forma de um substitutivo apresentado pela CCTCI – Comissão de Ciência e Tecnologia, Comunicação e Informática. O texto completo do PL 7.316 foi consolidado e atualizado de acordo com todas as emendas propostas e aprovadas pelas comissões e pelo relator, nos termos do substitutivo da CCTCI. Assim, constitui-se na mais atual proposição em tramitação no Congresso com respeito a normalização das disposições aplicáveis à certificação e assinatura digital.

O texto integral de todos os Projetos de Lei, Decretos e Medidas Provisórias apresentadas e discutidas neste capítulo encontra-se no Anexo I.

8.2.1. A validade jurídica do documento eletrônico e o novo Código Civil

O conceito de documento, também o eletrônico, não está vinculado à existência de uma assinatura aposta. Segundo GAIGER FERREIRA, "*A quase totalidade dos documentos está apócrifa, nem por isso sem autoria ou sem valor jurídico*" [93].

O novo Código Civil de 2002 (Lei nº 10.406 de 2002), apesar de não mencionar nenhum preceito disciplinando a certificação digital, ampara totalmente os documentos eletrônicos, pois os mesmos podem receber qualquer fato jurídico da mesma forma que os documentos tradicionais. As assinaturas eletrônicas não são assinaturas no sentido formal e legal, mas hoje são bastante populares e aceitas pela sociedade. De acordo com a nossa legislação "*não há forma especial para exprimir a vontade, quando a lei não exigir expressamente*" (art. 107 do Código Civil de 2002). Já as assinaturas digitais são distintas das assinaturas eletrônicas – são assinaturas formais por disposição legal (art. 1º, MP 2.200-2) e por ter amparo na técnica de criptografia assimétrica, o que garante os requisitos de autenticidade e integridade. O Novo Código Civil também dispõe em seu art. 219 que "*as declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários*", texto idêntico ao do art. 131 do Código de 1.916. Também o art. 225, dispõe que "*as reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão*".

O contrato eletrônico está sujeito a todas as normas previstas no Código Civil. Assim, de acordo com o art. 104, a validade do negócio jurídico eletrônico requer agente capaz, objeto lícito e forma não vedada em lei. Os contratos de adesão, tipicamente utilizados na Internet, tem previsão legal no art. 424, acrescentando que "*é lícito às partes estipular contratos atípicos, observadas as normas gerais fixadas neste Código*" (art. 425). De acordo com o art. 187, é ato ilícito o exercício de um direito além dos limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes. Isso também não exclui as hipóteses de invalidade prevista nos artigos de número 166 a 184. A incapacidade de uma das partes torna nulo o negócio jurídico. A capacidade relativa ou o erro – freqüente em negócios feitos à distância – podem dar causa à anulação (art. 171) [93].

Para se garantir a validade do negócio jurídico realizado de forma eletrônica, a utilização e popularização dos certificados digitais atenderá à identificação e a capacidade (agente capaz) para a realização de uma contratação (requisito autenticidade). Através da assinatura digital e da utilização de uma infra-estrutura de chaves públicas, pode-se garantir a não adulteração do contrato eletrônico a partir da comparação entre os "resumos" (*hash*), como foi demonstrado nos capítulos 5 e 6 desse trabalho (requisito integridade). Adicionalmente, a utilização de uma Autoridade de Datação ou carimbo de tempo, possibilita saber com exatidão a data e hora em que o documento foi assinado digitalmente (requisito tempestividade).

Os documentos eletrônicos e a sua possibilidade de contratação "virtual", constituem uma nova realidade que surgiu naturalmente do avanço tecnológico da sociedade em que vivemos. Cabe ao Direito o desafio de acompanhar a inovação tecnológica, disciplinando e normatizando a certificação digital e a utilização de documentos eletrônicos nos negócios jurídicos. Para que se produzam os efeitos previstos nos artigos 219 e 221 do novo Código Civil, as assinaturas digitais devem seguir os requisitos previstos na MP 2.200-2 de 2001 e no PL 7.316 de 2002, caso o mesmo venha a substituí-la.

8.2.2. A Legislação e as Proposições comentadas

Os Projetos de Lei inicialmente discutidos, tratam o assunto de documentos eletrônicos e sua integridade de maneira muito simplista (PL 2.644) ou através de conceitos equivocados e obsoletos (PL 3.173 e 4.734). O PL 1.532 guarda semelhança com a legislação a respeito da utilização de microfilmes, que são muito diferentes dos documentos eletrônicos

digitais. Com os conceitos equivocados, é claro que fica muito difícil garantir a integridade e “indelebilidade” (*sic*) dos documentos eletrônicos, conforme citado nos PL 3.173 e 1.532.

No entanto, o PL 1.483 teve o mérito de ter iniciado uma discussão acerca da utilização da fatura eletrônica e da assinatura digital, já indicando que o comércio eletrônico e a validade jurídica dos documentos eletrônicos poderiam estar bastante relacionados. O PL 1.589 trata de ambos os assuntos – assinatura digital e comércio eletrônico. Desenvolvido pela OAB, tem um bom detalhamento técnico e jurídico, bem superior às iniciativas anteriores. Os Projetos 1.483 e 1.589, dentre outros, foram apensados ao PL 4.906 de 2001 que trata de comércio eletrônico e baseia-se na lei modelo da UNCITRAL. Nesse cenário, o Comitê Executivo de Comércio Eletrônico criado em 2000, aprova sua primeira resolução em agosto de 2001, especificando os coordenadores dos sub-comitês, dentre outras providências. Porém, o comitê teve resultados ínfimos e o projeto está parado na Mesa Diretora da Câmara dos Deputados desde o final de 2001.

Com a experiência anterior da ICP-Gov, o Governo edita em 2001 a MP 2.200 instituindo a Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), com o objetivo principal de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica. A Medida Provisória 2.200 de 2001, com redação confusa e alguns artigos controversos, chega a ser reeditada por duas vezes (MP 2.200-1 e MP 2.200-2). Em razão da EC 32 de 2001, atualmente a MP 2.200-2 vigora com força de lei.

Ao final de 2002, o Poder Executivo tentou melhorar a MP 2.200 e também disciplinar o uso de assinaturas eletrônicas e a prestação dos serviços de certificação com o PL 7.316, um texto muito mais claro e abrangente que a Medida Provisória em vigor. Sem dúvida, foi um projeto muito discutido e inclusive já possui um substitutivo com parecer favorável que encontra-se parado desde o final de 2005 na CCJC.

Quanto ao comércio eletrônico, apenas no final de 2004, após um longo período sem debates, o Congresso Nacional e o governo retomaram a discussão sobre a regulamentação do comércio eletrônico no País, com a reinstalação do Comitê Executivo de Comércio Eletrônico. Infelizmente, com a instauração da CPI dos Correios em 2005, iniciou-se uma longa crise política que ainda não chegou ao fim.

Ainda em 2005, o Senador Pedro Simon, propôs projeto semelhante aos projetos 1.532 e 3.173, no entanto mais coerente e e apoiado na MP 2.200-2, a fim de garantir autenticidade e valor jurídico aos documentos eletrônicos no âmbito dos órgãos públicos federais, estaduais e municipais. Outra iniciativa que vale mencionar está relacionada à

inclusão do e-mail como prova documental, estabelecendo a presunção de sua autenticidade (PL 6.693 de 2006).

A seguir será realizada uma análise mais detalhada das proposições anteriormente citadas no Capítulo 7.

PROJETO DE LEI DA CÂMARA Nº 2.644 DE 11 DE DEZEMBRO DE 1996

O projeto 2.644 da Câmara dos Deputados dispõe sobre a elaboração, o arquivamento e o uso de documentos eletrônicos. Esse projeto de lei foi a primeira iniciativa legislativa diretamente relacionada à questão dos documentos eletrônicos. Excluindo-se os artigos 7 e 8 que tratam respectivamente da data de entrada em vigor da lei e da revogação das disposições em contrário, este projeto possui seis artigos referentes ao tema documento eletrônico. O art. 1º define de forma genérica um documento eletrônico. Já o art. 2º tenta estabelecer o conceito de documento original e de seus requisitos mencionando o uso de assinatura eletrônica. Esse projeto não deixa claro o que se pode considerar uma assinatura eletrônica, bem como quais seriam os seus requisitos e como poderiam ser garantidas a autenticidade e a integridade também mencionadas nesse artigo. O art. 4º prevê a possibilidade de cópia fiel em papel, sem mencionar os meios que poderiam assegurar a sua integridade. O art. 5º, por sua vez, trata da obscura figura do "administrador de recursos computacionais" e o art. 6º das penalidades envolvidas no tratamento dos documentos eletrônicos.

Percebe-se de maneira geral, um projeto muito simplista e abstrato para um tema relativamente complexo. Além disso, é distante do cidadão comum, com pouca contribuição para a popularização do uso dos documentos eletrônicos que tenta normatizar.

PROJETO DE LEI DO SENADO Nº 3.173 DE 26 DE MAIO DE 1997

Esse projeto é originário do PLS – 22 de 1996 e dispõe sobre os documentos produzidos e arquivados em meio eletrônico. Autoriza o arquivamento eletrônico de documentos por empresas privadas e órgãos da Administração Pública, desde que utilizado um sistema de gerenciamento eletrônico (para busca e indexação) e determina também que o arquivamento seja regulamentado por decreto específico. Ao mesmo tempo em que faculta a eliminação dos originais arquivados eletronicamente (art. 1º, § 2) dispõe que "*as dúvidas sobre as reproduções obtidas do acervo eletrônico deverão ser dirimidas [...] pelos respectivos originais*". Ainda no art. 1º, o parágrafo 3 afirma que "*o meio eletrônico utilizado*

deverá garantir a autenticidade, a indelibilidade (sic) e a confidencialidade dos documentos [...]".

Ao obrigar (art. 2º, § 1) a utilização de um sistema de indexação, esse projeto com certeza já encontra resistência principalmente no âmbito privado. Ao tentar garantir os requisitos de integridade, autenticidade e confidencialidade de forma equivocada, através do meio utilizado, nos remete as "tentativas iniciais de obtenção de um documento eletrônico imputável", assunto bastante discutido no Capítulo 3 desse trabalho. Atualmente, esse projeto encontra-se na Mesa Diretora da Câmara dos Deputados, com recurso de solicitação para apreciação no Plenário desde 2001 e tem grandes chances de não ser apreciado pelo seu caráter equivocado e obsoleto.

PROJETO DE LEI DA CÂMARA Nº 4.734 DE 12 DE AGOSTO DE 1998

Esse projeto de lei visa incluir um artigo (art. 7A) à lei nº 6.015 de 31 de dezembro de 1973, mais conhecida como Lei de Registros Públicos. Esse artigo faculta a utilização de discos ópticos ou optomagnéticos para escrituração dos registros públicos, sem prejuízo à utilização dos métodos tradicionais. É de se considerar importante a informatização dos registros públicos, inclusive os de escrituração. Entretanto, embora o artigo 7A mencione que devem ser observadas as disposições do capítulo V da lei 6.015, que trata da conservação, ordem e segurança dos arquivos, nada se menciona sobre como obter esses requisitos a partir do uso de discos ópticos ou optomagnéticos.

Há de se ressaltar que os discos optomagnéticos são regraváveis e há uma grande diversidade de tipos de discos ópticos, muitos também regraváveis e mesmo aqueles do tipo WORM, podem ter seus dados alterados dependendo de como forem utilizados (recurso de gravação em sessões múltiplas). Em relação às disposições do capítulo V da lei 6.015, seria oportuno mencionar que a forma de obtenção dos requisitos de autenticidade, integridade, disponibilidade e segurança dos arquivos armazenados em meio eletrônico digital, é bem diversa daquela utilizada para os documentos tradicionais em papel (vide seção 3.5 desse trabalho).

Por fim, o autor do projeto de lei menciona em sua justificativa a utilização do CD-ROM e do disquete, o que realmente comprova o caráter de inadequação e obsolescência desse projeto de lei.

PROJETO DE LEI DA CÂMARA Nº 1.483 DE 12 DE AGOSTO DE 1999

Esse projeto institui a fatura eletrônica e a assinatura digital nas transações de comércio eletrônico. Constitui-se de apenas dois artigos e em relação à assinatura digital, tem por objetivo a sua validação para utilização no comércio eletrônico. Propõe que o reconhecimento da assinatura seja feito por órgão público, porém não especifica qual órgão, nem o procedimento a ser adotado. Segundo o parágrafo único, garante-se ainda o direito de fiscalização dos registros disponíveis, o que no mínimo pode ser considerado um ponto de conflito ou de dupla interpretação, na medida em que poderia dar margem que órgãos federais tivessem acesso a dados sigilosos relacionados à técnica de assinatura digital utilizada, ou até mesmo alguma forma de controle dos documentos submetidos à certificação.

Apesar de ser muito sucinto, o PL 1.483 tem o mérito de ter iniciado um processo de discussão no âmbito do Poder Legislativo sobre uma regulamentação que estabeleça e discipline a utilização da assinatura digital no Brasil.

PROJETO DE LEI DA CÂMARA Nº 1.532 DE 19 DE AGOSTO DE 1999

O projeto de lei nº 1.532, de 1999, dispõe sobre a validade dos documentos públicos e particulares elaborados ou arquivados em meio eletromagnético que preserve a sua integridade. Para tanto, esse projeto já em seu art. 1º § único tenta garantir "*a segurança, a autenticidade, a nitidez, a indelebilidade* (sic) *e a confidencialidade dos documentos, protegendo-os contra todo acesso, uso, alteração, reprodução e destruição não autorizados*" através do meio eletrônico utilizado. Ora, já analisamos que somente através do meio utilizado não é possível obter tais propriedades para um documento eletrônico digital.

O texto desse projeto é semelhante à lei nº 5.433, de 8 de maio de 1968, que regula a microfilmagem de documentos, tecnologia hoje considerada obsoleta, mas que foi largamente utilizada no passado para armazenamento de documentos. Se a microfilmagem garantia a validade jurídica dos documentos submetidos a esse procedimento, através da regulamentação da lei acima citada, não se pode dizer o mesmo dos documentos eletrônicos digitais. Para garantir a validade jurídica dos documentos digitais é necessária a utilização de técnicas que garantam a sua integridade e autenticidade, hoje possíveis através do uso de assinatura e certificados digitais, com a chancela de uma autoridade certificadora, como por exemplo a ICP-Brasil. Esse projeto ainda está em tramitação e, em princípio, será apresentado

um substitutivo, mais adequado a atual realidade, embora não tenha sido possível obter o conteúdo do mesmo.

PROJETO DE LEI DA CÂMARA Nº 1.589 DE 31 DE AGOSTO DE 1999

Esse projeto dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e foi elaborado a partir de um anteprojeto de lei desenvolvido pela comissão especial de informática da OAB de São Paulo e apresentado pelo Dep. Luciano Pizzato. Trata do assunto com muito mais profundidade e maior detalhamento técnico e jurídico do que as iniciativas anteriores. O projeto tenta disciplinar o comércio eletrônico, bem como a utilização de documentos eletrônicos com validade jurídica.

Esse projeto define explicitamente como original de documento eletrônico aquele assinado por meio de sistema criptográfico de chaves-públicas (se esta puder ter sua autenticidade verificada) e como cópia, o impresso a partir do original eletrônico. Entretanto, em nenhum artigo é dada uma definição ou conceito do que se considera um documento eletrônico. Mas isso não chega a impactar negativamente o projeto, pois o mesmo trata de todos os princípios da tecnologia relacionados à assinatura digital, inclusive as autoridades certificadoras e a autenticidade de chaves feita por tabelião (podemos aqui considerar a idéia do cartório digital trabalhando com "*cybernotários*"). Estabelece também responsabilidades, competências e sanções penais das entidades envolvidas no processo de certificação eletrônica.

Interessante observar que nos artigos 16 e 17, o projeto faz distinção entre a certificação da chave pública feita por tabelião e aquela feita por particular e certificada por uma autoridade certificadora privada. A distinção baseia-se na presunção da autenticidade perante terceiros garantindo a sua autenticidade na certificação por tabelião. Já na assinatura feita por particular, nenhum terceiro fica obrigado a aceitar a autenticidade de um documento eletrônico, a não ser que assim deseje. No art. 18 afirma que "*a autenticidade da chave pública poderá ser provada por todos os meios de direito, vedada a prova exclusivamente testemunhal*". Esse artigo é interessante pois deixa a cargo do Judiciário definir a eficácia probatória de um documento assinado com determinada chave pública e não somente se respalda na tecnologia empregada, que eventualmente – embora difícil – possa ser fraudada.

Ao buscar a garantia da autenticidade perante terceiros junto a um serviço notarial, o projeto mantém equivalência com a situação atual dos documentos dotados de "fé pública", uma vez que a responsabilidade da autoridade certificadora permanece vinculada ao poder

público e não sob o domínio de qualquer entidade particular. Isso na teoria é muito interessante, entretanto na prática o projeto não observa as questões técnicas, principalmente àquelas relacionadas a real capacidade de um serviço notarial para controlar o uso de suas próprias chaves na certificação da autenticidade das chaves públicas apresentadas por seus clientes. É mais provável que a atribuição da garantia de autenticidade dos documentos eletrônicos caiba às entidades que detém a tecnologia de certificação digital, ou seja, as próprias autoridades certificadoras.

O art. 26 trata das informações mínimas que um certificado digital deve conter. Além dessas informações seria interessante a inclusão do prazo de validade do certificado e de seu número de série, informações essas constantes no padrão X.509 desde a sua primeira versão. O projeto estipula que caso não haja informação do prazo de validade do certificado, a validade é de 2 anos contados a partir de sua criação. A falta dessas informações tão importantes para um certificado digital (prazo e número de série) por si só deveria tornar o certificado inválido, pois o mesmo não segue os requisitos mínimos especificados pelo padrão X.509. O projeto ao dispor que os signatários presumem a data do documento como verdadeira (art. 19), não sugere a utilização de uma autoridade de carimbo de tempo ("*Time Stamping Authority*"), forma mais eficiente e segura de garantir o requisito da tempestividade.

Outra questão está na responsabilidade atribuída ao Ministério da Ciência e Tecnologia para certificar a segurança e a confiabilidade de programas e sistemas utilizados na geração de chaves criptográficas (art. 30). Seria mais democrático, se essa certificação fosse realizada por entidade especializada autorizada "*ad hoc*" para essa finalidade, a qual poderia perfeitamente suprir esse requisito.

O capítulo VI, segundo o art. 13, dispõe que "*aplicam-se ao comércio eletrônico as normas de defesa e proteção do consumidor*". Assim, o projeto trata de um assunto de relevante importância para o consumidor, pois sabe-se que até bem pouco tempo atrás os bancos não eram obrigados a seguir o código de defesa do consumidor, sendo esta uma conquista recente da sociedade brasileira.

Apesar de alguns questionamentos acima descritos, esse projeto trata de questões técnicas e jurídicas importantes relacionadas ao comércio eletrônico e à validade de um documento eletrônico. Esse projeto tem o grande mérito de levantar essas questões e assim propor a discussão com os vários setores da sociedade, inclusive o cidadão comum que realiza compras na Internet e que pode assim beneficiar-se de forma positiva com a normalização dessa matéria.

PROJETO DE LEI DA CÂMARA Nº 2.589 DE 15 DE MARÇO DE 2000

Esse projeto de lei altera o Código de Processo Civil de forma a admitir as decisões em mídia eletrônica entre as suscetíveis de prova na divergência de jurisprudência no âmbito do Superior Tribunal de Justiça (STJ). Iniciativa plenamente válida, pois as decisões já foram tomadas e simplesmente encontram-se em formato eletrônico (inclusive na Internet). Este projeto permite citá-las em caso de divergência jurisprudencial e foi recentemente (19/07/2006) encaminhado à sanção presidencial e não há razões para ser vetado.

PROJETO DE LEI DO SENADO Nº 4.906 DE 21 DE JUNHO 2001

Esse projeto dispõe sobre comércio eletrônico e ao mesmo foram apensados os PL 1483/1999, PL 1589/1999, PL 6965/2002 e PL 7093/2002 por tratarem de assunto correlato. Esse projeto toma como base a lei modelo proposta pela UNCITRAL, e assim trata do comércio eletrônico de forma neutra tecnologicamente sem mencionar características técnicas, nem mesmo como seriam obtidas as garantias de integridade e autenticidade das mensagens eletrônicas. Na verdade, tenta estabelecer regras básicas para o comércio eletrônico como tem ocorrido de forma empírica hoje em dia, mesmo sem legislação apropriada.

Conforme estabelece o art. 2º, inciso I, define-se mensagem eletrônica como sendo a "*informação gerada, enviada, recebida, armazenada ou comunicada por meios eletrônicos, ópticos, opto-eletrônicos ou similares*". Essa redação pode levar ao equivocado entendimento de que seria considerado documento eletrônico a informação simplesmente transmitida eletronicamente. Mas parece senso comum que a definição de mensagem eletrônica contém a definição de documento eletrônico.

Embora seja um projeto interessante, a partir do momento que traz um certo grau de normalização para o comércio eletrônico e possibilita inovações tecnológicas sem alteração da própria lei, as questões técnicas teriam que ser tratadas por regulamentação complementar.

O projeto é direcionado para o comércio eletrônico e dá pouca ênfase a questão da assinatura digital. Em seu art. 7º § único, o projeto abre um precedente para que o método de identificação de uma pessoa seja acordado entre as partes. Não indicando uma técnica a ser utilizada, deixa sob responsabilidade das partes a obrigação de ter conhecimento suficiente para estipular a forma como irão autenticar a operação. Se o método acordado não for adequado e não conseguir garantir os requisitos mínimos de integridade e autenticidade de

uma transação, poderá ser fraudado por uma das partes, ou até mesmo por terceiros, o que seria prejudicial para ambas as partes.

Como a este projeto foi apensado o PL 1589/1999, que trata do assunto com mais profundidade e detalhamento técnico, é de se esperar que o mesmo receba emendas ou até mesmo um substitutivo em razão de estar sendo discutido no âmbito do Comitê Executivo de Comércio Eletrônico reinstaurado em 2004, conforme já citado no Capítulo 7 deste trabalho.

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001
DECRETO Nº 3.872, DE 18 DE JULHO DE 2001

A MP 2.200 foi editada inicialmente em 28 de junho de 2001 e instituiu a Infra-estrutura de Chaves Públicas Brasileira, a ICP-Brasil com objetivo de "*garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações que utilizem certificados digitais*." (art. 1º). Estabeleceu como autoridade gestora de políticas um Comitê Gestor, vinculado à Casa Civil da Presidência da República, composto por membros da sociedade civil e representantes de diversos órgãos públicos indicados por seus titulares (art. 3º). A ICP-Brasil é composta de uma única Autoridade Certificadora raiz, ACs intermediárias e Autoridades de Registro (ARs). O art. 7º institui o Instituto Nacional de Tecnologia da Informação (ITI), como a AC raiz da ICP-Brasil.

Em seu art. 4º, estabelece que o Comitê Gestor será assessorado e receberá apoio técnico do CEPESC – Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações. O CEPESC nasceu dos trabalhos de pesquisa na área da criptografia do extinto SNI – Serviço Nacional de Informações e hoje é parte integrante da estrutura do Departamento de Tecnologia da Abin - Agência Brasileira de Inteligência. O art. 8º, com redação um pouco confusa determina que às ACs "*compete [...] gerenciar os certificados e as correspondentes chaves criptográficas*". Ora, o usuário que quiser emitir um certificado válido para a ICP-Brasil, é obrigado a confiar no ITI e no CEPESC, inclusive em relação gerenciamento de suas chaves ? Inclusive sua chave privada ? Sem contar que o ITI pode na forma da lei contratar serviços de terceiros (art. 7º, § único). Caso haja algum problema, segundo o inciso IV do art. 5º, cabe ao próprio Comitê Gestor exercer as atividades auditoria e fiscalização da AC raiz e seus prestadores de serviço.

Na verdade, a MP 2.200 ignorou os projetos de lei que há um razoável tempo tramitam no Congresso Nacional sobre a normalização de documentos eletrônicos e

assinaturas digitais, e emitiu às pressas uma MP com vários pontos polêmicos, deixando os usuários sem opção de escolha, caso a mesma venha a se consolidar no futuro.

A resposta veio rápida. A MP foi reeditada em 27 de julho de 2001 (MP 2.200-1) e corrigiu algumas discrepâncias. O art. 8º tem redação mais clara e foi incluído um parágrafo onde estabelece que o par de chaves criptográficas será gerado sempre pelo próprio titular, sendo a chave privada de seu exclusivo controle, uso e conhecimento. O art. 9º, determina que os usuários devem ser identificados e cadastrados comparecendo a uma AR (identificação presencial). Vários artigos foram reescritos a fim de dar maior clareza ao leitor (art. 5º, 6º, 11). O art. 5º, inciso VII, que trata de políticas de ICP externas, acrescenta que seja observado "*o disposto em tratados, acordos ou atos internacionais*". Já o art. 13 original foi suprimido, uma vez que não acrescentava nada de relevante ao assunto tratado pela MP.

Muito importante também foi a inclusão de parágrafos no art. 12 que estabelecem que os documentos certificados pela ICP-Brasil "*presumem-se*" verdadeiros (§ 1º), não obstando qualquer outro meio de comprovação de autoria e integridade de documentos eletrônicos, inclusive aqueles certificados fora da ICP-Brasil desde que admitido como válido pelas partes (§ 2). Assim, tentou-se aproximar a MP do tratamento de autoria e eventual litígio presente no Código Civil e no Código de Processo Civil. Por fim o art. 14, além da contratação de terceiros, permite a requisição de servidores, civis ou militares, e empregados da Administração Pública Federal direta ou indireta.

Novamente, em 24 de agosto de 2001, o governo reeditou a Medida Provisória (MP 2.200-2). Percebe-se logo que o ITI foi transformado em autarquia vinculada ao Ministério da Ciência e Tecnologia (MCT). O art. 4º que tratava do assessoramento do CEPESC foi suprimido. Entretanto, o Decreto 3.872 de 18 de julho de 2001 continua vigente e estabelece em seu art. 5º que "*o Comitê Gestor da ICP-Brasil estabelecerá a forma pela qual lhe será prestada assessoria pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações – CEPESC*". Outros acréscimos são o art.14 que afirma que o ITI pode aplicar sanções e penalidades na forma da lei e o art. 15 que dispõe de uma estrutura básica para o ITI (Uma Presidência, uma Diretoria de TI, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria Geral, que enquanto não for implantada, terá como representante a AGU – Advocacia Geral da União, segundo o art. 18). A transformação do ITI em autarquia, permitiu ao Poder Executivo transferir para o mesmo, o acervo técnico e patrimonial e as dotações orçamentárias consignadas ao MCT. Isso permitiu que o ITI recebesse recursos do Tesouro Nacional (vide Mensagem 268/06, Anexo I).

Embora a MP 2.200 e suas reedições tenham trazido importantes fundamentos e amparo legal à utilização da assinatura digital, esse assunto deve ser mais amplamente debatido para que algumas questões controversas sejam resolvidas de forma a atender e beneficiar a todos os usuários dessa tecnologia. Entre essas questões cabe mencionar:

- A falta de uma Autoridade de Datação ou carimbo de tempo (*Time Stamping Authority*), fundamental para se garantir o requisito de tempestividade para um documento assinado digitalmente;
- O mesmo tratamento dado aos documentos públicos ou particulares – "*para todos os fins legais*" – conforme dispõe a MP em seu art. 10.
- O certificado emitido pela ICP-BR é de uso geral e irrestrito, sendo que o uso inadequado ou o comprometimento da chave privada pode levar ao titular do certificado conseqüências de proporções drásticas.
- O gerenciamento da lista de certificados revogados (LCR) e a própria revogação de certificados, são outras duas questões de grande relevância. Nem sempre são de fácil solução e merecem mais atenção por parte da legislação.
- A identificação do titular de um certificado digital, caso não seja amparado por um procedimento eficaz por parte das ARs, pode se tornar o "calcanhar de Aquiles" de qualquer infra-estrutura, inclusive da ICP-Brasil.

PROJETO DE LEI DA CÂMARA Nº 7.316 DE 7 DE NOVEMBRO DE 2002 E SUBSTITUTIVO

Esse projeto de lei tem como objetivo substituir a MP 2.200-2 no que diz respeito ao uso de assinaturas eletrônicas e a prestação de serviços de certificação digital. Percebe-se que é um projeto mais evoluído e de redação mais clara, inclusive apresentando definições para esclarecer os diversos termos utilizados no decorrer do texto. Em seu art. 2º estabelece uma importante diferenciação entre assinatura eletrônica (como por exemplo a utilização de uma senha) e a assinatura eletrônica avançada baseada na utilização de um certificado digital. Em última análise, o "certificado qualificado" seria aquele emitido por prestador de serviços de certificação credenciado à ICP-Brasil (art. 2º § VII e IX) e a denominação de "certificado" não exigiria tal credenciamento. Ainda no art. 2º, § VII alínea "e" , trata inclusive de restrições ao âmbito de utilização do certificado, importante para evitar que o certificado se torne um instrumento de uso geral e irrestrito.

O art. 3º, dispõe que a prestação de serviços de certificação não se sujeita à prévia autorização pelo Poder Público, importante para democratizar a prestação desse tipo de serviço. Entretanto, cabe ressaltar que o art. 4º afirma "*que somente as assinaturas eletrônicas avançadas têm o mesmo valor jurídico e probante da assinatura manuscrita*". Dado que a assinatura eletrônica avançada tem como pré-requisito (art 2 § II, alínea c) estar "*baseada em certificado qualificado válido à época de sua aposição*" concluímos que o valor jurídico e probante somente é garantido ao certificado digital emitido por prestador de serviços de certificação credenciado à ICP-Brasil nos termos do art 5, que impõe o cumprimento de diversos requisitos. Todavia, não serão negados os efeitos jurídicos, nem será excluída como meio de prova, uma assinatura eletrônica que não estiver baseada em certificado qualificado, desde que admitida por ambas as partes como válida (art. 4º § 3). O art. 6º trata das condições de credenciamento de provedores de serviço de certificação de data e hora, bem como de outros serviços e aplicações de suporte, embora não relacione diretamente a certificação à exigência de um serviço de "carimbo de tempo", como seria importante para se garantir o requisito de tempestividade.

O projeto trata também das responsabilidades dos prestadores de serviço de certificação (art. 10), infrações, multas e aplicação do Código de Defesa do Consumidor (art 15), incluindo a necessidade do prestador informar as medidas de segurança que devem ser adotadas pelos usuários para com os seus certificados e chaves, em especial a sua chave privada (art. 8º). No art. 14, assegura que o certificado emitido no exterior seja considerado um "certificado", podendo ser considerado um "certificado qualificado" desde que sejam realizados acordos, tratados ou atos internacionais, observando-se o princípio de reciprocidade. Esse projeto de lei em seu art. 18, não dispensa a manutenção em papel ou microfilme dos livros de registros públicos na forma da legislação vigente (Lei 6.065/1973) e mantém as competências do Comitê Gestor da ICP-Brasil na forma da MP 2.200-2, salvo disposição contrária. Muito importante é a exigência de contratação de seguro pelos prestadores de serviço para cobertura da responsabilidade civil relativa à atividade de certificação (art. 25). Esse dispositivo assegura aos usuários maiores garantias de ressarcimento em um eventual dano financeiro causado pela entidade certificadora.

Ressalta-se que o objetivo inicial do projeto de lei do Executivo era consolidar as disposições aplicáveis à certificação e assinatura digital, bem como dar um tratamento legislativo adequado a algumas questões não tratadas pela MP 2.200-2. Inicialmente, o PL 7.316 oriundo do Poder Executivo, continha 20 artigos e nas comissões recebeu substitutivo

da CCTCI (Comissão de Ciência e Tecnologia, Comunicação e Informática), além de inúmeras emendas tanto da CCTCI como da CCJC (Comissão de Constituição, Justiça e Cidadania). Com o substitutivo, que realizou diversas alterações e inclusões, o PL passou a dispor de 49 artigos. A partir do substitutivo, novamente foram apresentadas emendas, inclusive do relator. Após a consolidação das emendas aprovadas, atualmente o PL trata do assunto em 52 artigos, com um nível de detalhamento e esclarecimento bem mais significativo que o PL original do Executivo.

No PL consolidado, dentre as alterações efetuadas, podemos citar as novas definições de assinatura eletrônica, certificado qualificado e documento eletrônico (art 2), que colocam o projeto de lei em sintonia com a legislação internacional, em especial com a Diretriz da Comunidade Européia. O substitutivo elucida ainda a relação inequívoca entre a assinatura eletrônica e seu titular e explicita a data de início e fim da validade do correspondente certificado como informação obrigatória no "certificado qualificado" (art. 2º e 3º). Ainda no art. 2º, é incluído um parágrafo único, que equipara a pessoa jurídica, para os fins do inciso IX, aqueles que exercem serviços notariais, nos termos do art. 236 da CF. Em seu art. 5º dispõe que as assinaturas eletrônicas têm o mesmo valor jurídico e probante das assinaturas manuscritas, de acordo com o art. 219 do novo Código Civil de 2002. Há um novo capítulo (Título I, Capítulo III) que trata dos certificados digitais, atribuindo a posse da chave criptográfica ao seu possuidor, que será responsável por sua geração e guarda, respondendo pelo uso exclusivo da chave de criação de assinatura. O §4 do art. 8º explicita que os dados do certificado são públicos e disponíveis a qualquer interessado, o que não era exatamente o que dizia a redação anterior, que afirmava que "*os certificados podiam ser conferidos pelo público apenas quando consentido pelo seu titular*". O Substitutivo trata ainda da ICP-Brasil e de seu Comitê Gestor, definindo sua composição e suas competências (Título II, Cap I e II), bem como seu relacionamento com o Instituto Nacional de Tecnologia da Informação – ITI, cujo papel de gerente técnico do sistema é detalhado e reforçado (Título II, Cap III).

O Substitutivo reconhece, no âmbito do sistema nacional de certificação digital, o papel de destaque do Observatório Nacional – órgão do Ministério da Ciência e Tecnologia que mantém a hora legal brasileira – e sua importância na confiabilidade do sistema de certificação digital. Para tanto, o art. 22 estabelece que os prestadores de serviço de carimbo de tempo devem utilizar a hora oficial fornecida pelo Observatório Nacional, incluindo seus sinais primários de sincronização de freqüência e tempo.

No Capítulo III do Título III – Dos Deveres das Prestadoras de Serviços de Certificação – a versão consolidada obriga as autoridades de registro a prestarem informações ao usuário do sistema sobre os efeitos da certificação, sobre a forma de geração e uso das chaves criptográficas, bem como sobre os cuidados a serem tomados em sua guarda e manipulação (art. 32). É aplicável a legislação de defesa do consumidor e as normas processuais sobre a validade e prova documental à prestação de serviços de certificação e datação (art. 45).

O Capítulo VI introduz ainda, uma gradação de penas aplicáveis aos prestadores de serviços, criando diversas categorias de infração e penalidades no âmbito do sistema ICP-Brasil.

Interessante observar que as Autoridades Certificadoras (ACs), passam a ser conhecidas como prestadores de serviços de certificação (exceto no caso da AC raiz da ICP-Brasil) e as antigas Autoridades de Registro (ARs) passam a ser referenciadas como órgãos de registro (art. 48), embora essa alteração seja somente na nomenclatura utilizada. Já o art. 49, dispõe que a constituição de direitos e obrigações instrumentada em documento eletrônico que importem em transferência de domínio imobiliário ou envolvam interesse de incapazes, para ter validade perante terceiros, deve sujeitar-se às prescrições da legislação civil, processual e dos registros públicos em vigor. Por fim, revoga a MP 2.200-2 e convalida os atos praticados em sua vigência.

De uma maneira geral, o PL 7.316 consolidado traz inúmeras melhorias em relação a MP 2.200-2, muitas das quais já discutidas anteriormente. O PL trata em detalhes a prestação de serviços de certificação digital, incluindo o serviço de carimbo de tempo, seus requisitos e responsabilidades. Estabelece ainda normas sobre o uso de assinaturas eletrônicas e certificados digitais, versando sobre o papel exercido pela ICP-Brasil, pelo ITI e pelos prestadores de serviço de certificação e datação. Em vários aspectos tenta compatibilizar a utilização de assinaturas eletrônicas com a legislação existente, na medida em que não coloca nenhum óbice aos meios de prova e contestação hoje existentes. Além disso, estabelece regras para os componentes de aplicação e componentes técnicos (programas e dispositivos) e dispõe ainda sobre a manutenção/encerramento das atividades de certificação, estabelecendo também penalidades às eventuais infrações cometidas pelas entidades credenciadas.

Entretanto, a infra-estrutura proposta continua sendo de raiz única e com o objetivo de se obter um certificado qualificado e assim possuir uma assinatura eletrônica avançada, o usuário é “sugestionado” a requisitá-la perante um prestador de serviço

credenciado, ou seja, participante do sistema de certificação no âmbito da ICP-Brasil. Ao obter um certificado digital de outra entidade não participante da ICP-Brasil, obterá a possibilidade de assinar digitalmente um documento, que não necessariamente terá o mesmo valor jurídico e probante das assinaturas manuscritas (art. 5º), embora não sejam negados os seus efeitos jurídicos, desde que o certificado digital seja admitido como válido pelas partes ou aceito pela pessoa a quem seja oposto (art. 6º).

PROJETO DE LEI Nº 229 DE 22 DE JUNHO DE 2005

Esse projeto dispõe sobre a autenticidade e o valor jurídico e probatório de documentos produzidos, emitidos ou recebidos por órgãos públicos federais, estaduais e municipais, por meio eletrônico. A idéia de sua proposição é semelhante aos projetos 1.532 de 19 de agosto de 1999 e 3.173 de 26 de maio de 1997, entretanto encontra respaldo na MP 2.200-2 a fim de garantir a autenticidade e integridade dos documentos em questão. Ainda está em fase inicial de tramitação, sem relator designado. Entretanto, tem uma aceitação maior, é mais condizente com a atual realidade da certificação digital no Brasil e por isso tem mais chances de ser aprovado, após discussão nas duas Casas do Congresso Nacional. Como menciona uma MP, que hoje tem força de lei, em algum momento futuro deve sofrer emenda para se adequar a uma possível mudança na situação da normalização da certificação digital no Brasil.

PROJETO DE LEI Nº 6.693 DE 07 DE MARÇO DE 2006

Esta lei altera a redação do art. 375 da lei no 5.869, de 11 de janeiro de 1973 - Código de Processo Civil. Dispõe que conforme o telegrama e o radiograma, o e-mail seja presumido conforme o original, provando a data de sua expedição e do recebimento pelo destinatário. Essa proposição ainda deverá receber parecer conclusivo pela CCJC, onde encontra-se atualmente. Mas deve ficar claro que o e-mail é considerado um documento eletrônico digital e por isso deve ser tratado como tal. Caso o e-mail possua uma assinatura digital válida fica mais fácil e isenta a comprovação de sua autenticidade e integridade; caso contrário, somente uma perícia pode atestar o seu grau de legitimidade, cabendo a justiça deliberar sobre a sua originalidade e integridade.

Nesse sentido, a exemplo de jurisprudência, o Tribunal Superior do Trabalho, em 27 de maio de 2003, rejeitou o envio de petição recursal por meio de correio eletrônico, pois o considerou um mecanismo díspar em relação ao fac-símile, embasado na MP 2.200-2. "*O*

envio de recurso por correio eletrônico é juridicamente aceitável apenas se houver certificação digital reconhecida pela ICP-Brasil, nos termos da MP 2.200-2 de 2001”[94].

8.2.3. Outras questões relevantes

Após a análise mais detalhada da legislação apresentada, vimos que o Brasil ainda não possui um detalhamento jurídico vigente, e por vezes específico, de como deve ser tratada a questão dos documentos eletrônicos digitais. A MP 2.200-2, atualmente com força de lei, tenta normatizar o aspecto relacionado à validade jurídica dos documentos eletrônicos através da criação da ICP-Brasil, que de acordo com o seu art. 1º foi instituída com o objetivo de “*garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica [...]*”. O PL 7.316, na forma de substitutivo apresentado pelo relator, se for sancionado, ficará no lugar da MP 2.200-2 e irá convalidar os atos praticados na vigência da MP. É muito mais abrangente, traz melhorias evidentes e com certeza foi muito mais debatido e modificado através das comissões. Assim, embora tenha um caráter mais democrático que uma Medida Provisória, atualmente com força de lei pelas circunstâncias da EC 32 de 2001, a essência é a mesma da MP 2.200-2. A seguir serão comentadas algumas questões relevantes relacionadas a esses dois instrumentos normativos e ao processo de aceitação das assinaturas digitais pela sociedade de uma forma geral.

A ICP Raiz única e o CEPESC na MP 2.200-2 e no PL 7.316

A ICP-Brasil ocupa lugar de destaque nas duas normas acima citadas. Ora, é através dessa infra-estrutura que se pretende dar validade jurídica aos documentos eletrônicos e disciplinar o uso de assinaturas eletrônicas e a prestação de serviços de certificação. A infra-estrutura de certificação é onerosa, sendo natural que a atividade de certificação seja considerada uma atividade comercial, com um vínculo estabelecido entre quem fornece e quem adquire um certificado.

Pelas normas citadas, todos os prestadores do serviço de certificação que quiserem ter a possibilidade de emitir um “certificado qualificado” e assim poderem fornecer aos seus usuários uma “assinatura avançada”, terão que seguir as normas estabelecidas pelo Comitê Gestor da ICP-Brasil, que continua sendo assessorado tecnicamente pelo CEPESC, órgão da ABIN (antigo SNI), a menos que o Decreto 3.872 seja revogado pelo Poder Executivo.

Como já foi comentado, o Brasil adotou um modelo centralista e hierárquico de ICP raiz única, que tem fortes influências do modelo adotado pela Alemanha. No início dos anos 90, uma iniciativa de se implementar um modelo centralista deu-se no âmbito do esforço de universalização do padrão PEM (*Privacy Enhanced Mail Standard*). O padrão PEM, incluía cifragem, autenticação e o uso de um sistema de chave pública e privada para garantir a privacidade e integridade na troca de mensagens eletrônicas de forma segura. Proposto pela IETF (*Internet Engineering Task Force*), o padrão fracassou devido a diversas dificuldades, a maioria delas decorrentes de obstáculos para se adequar sua esfera técnica à esfera jurídica [95].

A falta de "concorrência", pode comprometer a qualidade de um serviço fornecido pelo Estado, já que cabe ao próprio Comitê Gestor coordenado pelo Poder Executivo (MP art. 4º Inc. IV e art. 15, Inc. IV do PL 7.316 consolidado) auditar, homologar e fiscalizar a ICP-Brasil e seus prestadores de serviço.

Aos poucos alguns serviços públicos começam a ser oferecidos ao cidadão através da utilização de "certificados qualificados" emitidos pela ICP-Brasil, como por exemplo, alguns serviços ao contribuinte fornecidos pela Secretaria da Receita Federal. No futuro, quando a certificação digital for popular, caso o usuário adquira um certificado digital de uma empresa comercial e esta não esteja sob os auspícios da ICP-Brasil, os órgãos públicos terão possibilidade de aceitá-los ? Nesse caso, terá o usuário de um serviço público alguma outra opção de certificado, além daqueles emitidos pelos prestadores de serviço vinculados à ICP-Brasil ? Só o tempo dirá, pois a legislação vigente e a atual proposta futura (PL 7.316) não tocam diretamente no assunto.

Pode ser que esses obstáculos sejam superados na medida em que haja maior adesão da população à utilização da certificação digital. É possível que com o amadurecimento da tecnologia e a evolução das normas jurídicas, surjam acordos bilaterais que viabilizem a utilização da certificação cruzada. A certificação cruzada é aquela utilizada na identificação de chaves públicas entre duas autoridades certificadoras distintas, não pertencentes à mesma árvore de certificação. A partir de então, cada qual passa a ter o mesmo grau de confiança, e o usuário poderá solicitar um certificado da hierarquia de certificação de sua preferência, deixando de ser a certificação um serviço exclusivamente Estatal e monopolista.

A questão da Privacidade

Em um mundo globalizado e com vários tipos de relações sendo realizadas em ambientes "virtuais" como a Internet, a privacidade do usuário é muito importante. Quem gostaria de ter os seus dados pessoais divulgados pela internet, ou vendidos por quantias irrisórias em um DVD pirata ?

Pois bem, as resoluções do ITI de números 7, 11, 13, 28, 31, 35 e 41 – todas versando sobre os requisitos mínimos sobre as políticas de certificado na ICP-Brasil – determinam que inúmeras informações pessoais fossem obrigatoriamente informadas em campos denominados "*OtherName*". Em particular, a resolução 41, obriga a existência de 3 campos "*OtherName*", contendo o primeiro a data de nascimento do titular, o Cadastro de Pessoa Física (CPF) do titular, o número de Identificação Social NIS (PIS, PASEP ou CI), o número do Registro Geral RG do titular, as siglas do órgão expedidor do RG e respectiva UF; o segundo contendo o número do Cadastro Especifico do INSS (CEI) da pessoa física titular; o terceiro contendo o número de inscrição do Título de Eleitor, a Zona Eleitoral, a Seção e por fim, o município e a UF do Título de Eleitor.

Sabendo dessas questões, um usuário emitiria um "certificado qualificado" pela ICP-Brasil, contendo todas essas informações ? Seria realmente seguro ?

Como esses dados fazem parte do certificado digital do usuário e o seu conteúdo é público e passível de verificação por uma Autoridade Certificadora (AC), seria possível obtê-los através de um programa ou rotina especialmente projetado para esse fim ? A resposta é sim. Segundo CARNUT [96], não só é possível como ele nos mostra em seu artigo "Certificados Digitais Pseudônimos: Identificação Segura e Privacidade são Compatíveis" uma rotina escrita na linguagem "*Perl*" que extrai vários dados pessoais de uma AC real, mostrando-os na tela de forma descritiva e em formato fácil para importação em bancos de dados. Ressalta o autor que a rotina não é ilícita, pois "*não explora nenhuma vulnerabilidade obscura no servidor web ou na aplicação da AC, nem realiza nenhum tipo de acesso ilegal; simplesmente acessa a página tal como o navegador o faz, não disparando nenhum alarme de ataque na AC*" [96].

Prato cheio para falsários e estelionatários. Cabe ressaltar que a resolução 41 continha os requisitos mínimos sobre as políticas de certificado na ICP-Brasil (versão DOC-ICP-04), estava vigente até há pouco tempo, quando a resolução 42 em 18 de abril de 2006 aprovou a versão DOC-ICP-05. Esta última dispõe que os dados obrigatórios do campo "*OtherName*" são o nome completo do titular e a data de nascimento. Os demais campos são

opcionais a critério do usuário ou podem ser incluídos de acordo com a política específica de utilização do certificado.

É importante mencionar que a não-inclusão desses dados não prejudica em absoluto a utilização dos certificados digitais nem por parte dos usuários, nem das aplicações e serviços deles dependentes. Simplesmente preservam o sigilo de dados pessoais do titular, garantindo assim a sua privacidade.

A questão do não repúdio

A jurisprudência no Brasil tem atuado no sentido de considerar a segurança no meio eletrônico colocado a disposição dos usuários de "*home-banking*", comércio eletrônico, dentre outras modalidades de contratação virtual, como risco profissional do fornecedor desse tipo de serviço. Assim, aquele que se organiza para negociar por meio eletrônico profissionalmente, deve suportar o risco de identificação e imputação errônea de uma vontade negocial. Um "terceiro" pode ter descoberto a senha, através de mecanismos ilícitos, e assim cabe ao fornecedor o risco e a prova da contratação e da vontade de pagamento, uma vez que o mesmo é quem conhece a segurança de seus sistemas e programas de computador [97].

Com a utilização da certificação digital, a MP 2.200-2 em seu art. 6º, parágrafo único, afirma que "*o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento*". Esse parágrafo, em conjunto com o art. 10 da citada MP, pode dar a interpretação de que o usuário não poderia repudiar o uso de sua chave privada na assinatura de um documento. Esse conceito é conhecido como não repúdio. Há de se lembrar de que nenhum sistema é totalmente imune às falhas, erros ou até mesmo fraudes. E o que dizer então da coação ? Como não seria repudiável uma situação de que o usuário utilizou sua chave privada para assinar um documento eletrônico sob a coação de uma arma ? Nessas situações, cabe ao usuário provar que não foi ele quem utilizou a sua chave privada para "assinar" um documento, ocorrendo uma inversão do ônus da prova. Observe que essa posição já é contrária à jurisprudência mencionada no início dessa seção.

Até mesmo no meio técnico especializado, há autores revendo sua posição em relação ao não repúdio. SCHNEIER [98], em seu livro "*Segurança.com – Segredos e mentiras sobre a proteção na vida digital*", refuta exatamente o conceito de não repúdio, exposto e defendido por ele em obra anterior. A questão do não repúdio é bastante controversa, tanto que o PL 7.316 consolidado, art. 8º § 2º, tem redação diferente da MP

2.200-2 ao tratar do par de chaves criptográficas, não delegando mais o controle das mesmas exclusivamente ao titular: "*O titular ou o responsável pelo uso do certificado gerará o par de chaves criptográficas e responderá pela guarda e pelo uso exclusivo da chave de criação de assinatura*".

Por fim, não se pode esquecer de que nem todos os usuários, ao usarem os seus certificados digitais, estarão conscientes de todos os aspectos (técnicos e legais) que envolvem o processo de certificação digital. Daí a importância da necessidade do prestador de serviços de certificação, informar as medidas de segurança que devem ser adotadas pelos usuários para com os seus certificados e chaves, em especial a guarda de chave privada (conforme já dispõe o art. 8º do PL 7.316 consolidado).

8.3. CONSIDERAÇÕES FINAIS

Esse capítulo deixa claro que os problemas técnicos relacionados aos requisitos para obtenção da validade jurídica dos documentos eletrônicos, podem ser superados com a adoção da criptografia assimétrica, de uma infra-estrutura de chaves públicas para emissão e validação de certificados digitais, além da aprovação de uma legislação coerente e pertinente com a realidade brasileira.

Infelizmente, grande parte dos projetos de lei analisados que tratam de normatizar o uso de documentos eletrônicos e assinaturas digitais, o fazem de maneira equivocada. Em conjunto com um Processo Legislativo moroso, com a pauta de votações invariavelmente trancada por Medidas Provisórias, essas iniciativas acabam esquecidas e se tornam obsoletas. Espera-se que o mesmo não aconteça aos importantes projetos de lei 4.906-A de 2001 e 7.316 de 2002, este último com o objetivo de substituir a MP 2.200-2 que entre outras providências, instituiu a ICP-Brasil. Uma forma de acelerar o processo legislativo, seria a aprovação da Proposta de Emenda à Constituição (PEC) nº 72 de 2005, que modifica o trâmite das medidas provisórias no Congresso Nacional [99]. A principal alteração da proposta é o dispositivo que prevê que uma medida provisória apenas ganhará força de lei, depois que seus requisitos constitucionais de urgência e relevância forem reconhecidos pelo Congresso. Pela regra atual, uma MP tem eficácia tão logo é assinada pelo presidente da República.

Apesar das questões técnicas discutidas anteriormente, o potencial usuário dos serviços de certificação digital da ICP-Brasil, não tem controle sobre as características e procedimentos técnicos que envolvem uma infra-estrutura de certificação digital. Entretanto, pode encontrar respaldo nas resoluções emitidas pelo Comitê Gestor da ICP-Brasil, em

especial as resoluções que tratam da Declaração de Práticas de Certificação da AC Raiz, da Política de Segurança da ICP-Brasil, dos Requisitos mínimos para as Políticas de Certificados e dos Requisitos mínimos para as Declarações de Práticas de Certificação. Além disso, diversas ações dirigidas pelo ITI, como a disponibilização do código fonte de aplicações para o usuário, a nacionalização da plataforma de certificação e a criação de um laboratório de ensaios e auditoria (LEA), tem por objetivo aumentar a transparência e confiança do usuário na infra-estrutura de certificação fornecida pela ICP-Brasil.

A popularização da certificação digital, também depende do custo dos dispositivos de armazenamento seguro de chaves e certificados, como os "*smart cards*" e "*tokens*". Os mesmos só serão mais acessíveis à população, se houver um esforço na sua padronização.

Por fim, cabe citar alguns serviços que se utilizam de certificados digitais que estão sendo disponibilizados para o cidadão ou para uma comunidade de usuários. Um dos pioneiros foi o serviço de atendimento virtual da Receita Federal, mais conhecido como "Receita 222", e hoje ampliado para o Centro Virtual de Atendimento ao Contribuinte da Secretaria da Receita Federal ou e-CAC. O acesso ao e-CAC é efetivado mediante a utilização de certificados digitais possibilitando, dentre outros procedimentos, a consulta e regularização das situações cadastral e fiscal dos contribuintes, a emissão de certidões e o acompanhamento da tramitação de processos fiscais [100].

Outro serviço importante é o SPB (Sistema de Pagamentos Brasileiro), que tem como função primordial a transferência de recursos entre pessoas, empresas e instituições financeiras [101]. Todas as operações do SPB são certificadas digitalmente e com isso, é possível que uma transferência de valor maior ou igual a 5 mil reais, seja processada quase que instantaneamente, por meio de uma TED (Transferência Eletrônica Disponível).

Pode-se citar também o SISPROUNI, sistema do ProUni (Programa Universidade para Todos). O ProUni tem como finalidade a concessão de bolsas de estudos integrais e parciais a estudantes de baixa renda, em cursos de graduação em instituições privadas [102]. O acesso dos mantenedores e coordenadores ao SISPROUNI, é feito exclusivamente por meio de certificados digitais. Outros sistemas que utilizam os certificados digitais são o DETRANNET (módulo para uso de Despachantes, Clínicas Médicas e Centros de Formação de Condutores) e o Programa Juro Zero de financiamento da micro e pequena empresa da FINEP [103], dentre outros.

Segundo o ITI, a título de exemplo, a Autoridade Certificadora da Caixa Econômica Federal, já emitiu mais de 15 mil certificados e estabeleceu convênios com

diversos tribunais incluindo o STF, STJ, TRT, TST e o TJDFT, com expectativa de superar a marca de 90 mil certificações até 2007, somente no âmbito do poder judiciário [104].

Recentemente, a Câmara dos Deputados afirmou que a partir da próxima legislatura, que se inicia em 15 de fevereiro de 2007, será adotado o sistema de assinatura digital. Atualmente, a Câmara já utiliza mensagens de correio eletrônico assinadas digitalmente, e com a definição iminente do formato de documentos digitais textuais, os parlamentares, a Mesa Diretora e os demais diretores de órgãos da casa deixarão de assinar documentos em papel, passando a autenticá-los eletronicamente.

Apesar desses esforços, conflitos começam a surgir em relação a “obrigatoriedade” de uso de certificados emitidos pela ICP-Brasil para acesso de determinados serviços, como o Sistema Integrado de Protocolização e Fluxo de Documentos Eletrônicos da Justiça do Trabalho (e-DOC), de acordo com a Instrução Normativa nº 28 de 2005 emitida pelo Tribunal Superior do Trabalho. A OAB, apresenta “pedido de providências” [105] ao Conselho Nacional de Justiça em razão da existência de certificados emitidos pela ICP própria da OAB (ICP-OAB), através do Provimento nº 97/2002, emitido pelo Conselho Federal e que de acordo com a citada Instrução Normativa, não poderiam ser utilizados para peticionamento eletrônico no sistema e-DOC.

9. CONCLUSÃO

Os documentos eletrônicos começaram a ser utilizados pouco tempo depois do surgimento dos primeiros computadores. Entretanto, seu uso só se tornou comum com a proliferação dos microcomputadores, e mais ainda, com o surgimento da internet, quando a adoção da tecnologia se viu estimulada, grande parte em razão das novas possibilidades de comunicação e interação, mas também em função dos valores econômicos e interesses comerciais envolvidos.

O desenvolvimento das técnicas de criptografia, em especial a criptografia assimétrica, permitiu o surgimento da assinatura digital de um documento eletrônico. Com base na utilização de certificados digitais, esse tipo de assinatura permite que se possa obter os requisitos de autenticidade e integridade de um documento ou mensagem eletrônica. A assinatura digital depende da existência de uma estrutura, denominada de Infra-estrutura de Chaves Públicas (ICP), que permite que as chaves públicas dos signatários possam ser verificadas e validadas.

O estabelecimento e o gerenciamento de uma infra-estrutura de certificação digital envolve tarefas complexas, muito além das técnicas de criptografia empregadas. A criptografia é apenas parte de um sistema maior onde coexistem pessoas, computadores, redes de comunicação e sistemas de informação operando sofisticados algoritmos. A aplicação prática das assinaturas digitais depende, em primeiro lugar, da confiança que os usuários depositam nas Autoridades Certificadoras (ACs) e seus procedimentos de segurança. As atividades técnicas, como por exemplo, a realização de auditoria e fiscalização das entidades certificadoras, a atualização dos programas utilizados com a utilização de algoritmos mais seguros e o acompanhamento da evolução tecnológica, devem ser sempre seguidas e observadas. Também está muito claro que o uso correto da tecnologia, por parte do usuário, é fundamental para que se garanta a segurança e a usabilidade de toda estrutura envolvida no processo de certificação digital.

Na questão jurídica, a legislação atual brasileira já vem sendo aplicada, através de adequação e adaptação, nas questões relacionadas aos documentos eletrônicos e à assinatura eletrônica, como por exemplo, em uma contratação eletrônica na Internet (comércio eletrônico). Apesar dessa jurisprudência, o avanço da tecnologia é rápido e o Processo Legislativo brasileiro não tem conseguido acompanhar a demanda por normas e instrumentos

jurídicos mais adequados a essa nova realidade. A regulamentação sobre o comércio eletrônico e a certificação digital deve ser semelhante às regras estabelecidas para o comércio no mundo real, considerando os aspectos virtuais e específicos da tecnologia.

Como foi visto, grande parte das proposições em tramitação no Congresso Nacional, trata equivocadamente os documentos eletrônicos e a manutenção de sua integridade e conseqüente validade jurídica. Aqueles projetos que são mais adequados, muitas vezes foram propostos pelo próprio Poder Executivo, trazem diversos pontos questionáveis e ainda são submetidos a um Processo Legislativo complexo e constantemente paralisado pelo excesso de Medidas Provisórias que trancam a pauta de votações no Congresso Nacional. Ao demorar para serem apreciados e sendo sobrepujados por outros projetos com regime de tramitação de urgência, acabam por perder o compasso com a tecnologia, tornando-se muitas vezes obsoletos e assim inadequados à tecnologia vigente.

Nesse ínterim, surge a Medida Provisória 2.200 e suas duas reedições, instituindo a infra-estrutura de chaves públicas brasileiras denominada de ICP-Brasil. Essa medida teve como objetivo principal, garantir a validade jurídica dos documentos eletrônicos assinados digitalmente, com o uso de certificados emitidos no âmbito da ICP-Brasil e ainda está em vigor em razão da EC 32 de 2001. Analisando as disposições contidas na MP 2.200-2 e as questões técnicas relacionadas ao funcionamento de uma ICP, diversas situações podem afetar o usuário de um certificado digital. Dentre elas, podemos citar: 1) Emissão de um certificado a partir de um procedimento inadequado de identificação do seu titular; 2) Falhas no gerenciamento e disponibilização das Listas de Certificados Revogados (LCRs); 3) Inexistência de uma Autoridade de Datação para garantir a tempestividade da assinatura digital; 4) Emissão de certificados de uso geral e irrestrito, já que qualquer erro técnico ou comprometimento da chave privada, pode ter conseqüências de proporções incalculáveis para o seu titular.

O projeto de lei 7.316 de 7 de novembro de 2002, já com seu texto consolidado na forma de um substitutivo apresentado pela CCTCI e emendado pela CCJC, tenta solucionar ou minimizar algumas das situações mencionadas anteriormente. Entre seus pontos positivos encontram-se: 1) A definição do Observatório Nacional como provedor de hora oficial para os prestadores de serviço de datação; 2) Definição clara de requisitos e responsabilidades na prestação de serviços de certificação digital; 3) Estabelecimento de penalidades às eventuais infrações cometidas pelas entidades credenciadas; 4) Menção a possibilidade de restringir o âmbito de utilização do certificado, evitando assim que o certificado fosse de uso amplo e

irrestrito; 5) Manutenção de contrato de seguro para coberta de responsabilidade civil relacionada à atividade de certificação. Embora o PL 7.316 tenha trazido inúmeras melhorias, a infra-estrutura proposta continua sendo de raiz única e há um artigo dispondo que "*somente as assinaturas eletrônicas avançadas têm o mesmo valor jurídico e probante da assinatura manuscrita*". As assinaturas avançadas têm como pré-requisito estarem baseadas em "certificados qualificados", que somente são emitidos por prestadores de serviços credenciados à ICP-Brasil.

Assim, caso o usuário queira que a sua assinatura digital tenha o mesmo valor jurídico e probante de sua assinatura manuscrita, fica claro que o mesmo não tem opção, a não ser obter um certificado de Autoridade Certificadora credenciada na ICP-Brasil.

Outro aspecto muito importante, diz respeito a irretratabilidade ou não repúdio em relação a aposição de assinatura digital em uma mensagem ou documento eletrônico. Com as assinaturas eletrônicas, atualmente o ônus da prova no caso de fraude ou de erro que provoque prejuízos é, por jurisprudência, do fornecedor do serviço. As características técnicas dos certificados digitais, em conjunto com as normas legais hoje existentes, podem fazer com que haja a inversão do ônus da prova. Isso torna o usuário da certificação digital (contratante de um serviço), único responsável pela utilização indevida de sua assinatura digital, mesmo que tenha ocorrido algum erro, falha técnica ou até mesmo fraude, já que é impossível garantir um sistema totalmente seguro e perfeito. Isso parece não estar sendo levado em consideração, principalmente por entidades diretamente interessadas nessa inversão do ônus da prova, o que é um risco que o usuário pode vir a assumir ao utilizar seu certificado digital.

Mesmo com todas essas questões, o uso de assinaturas digitais em conjunto com uma infra-estrutura de chaves públicas confiável, tende a aumentar o nível de segurança em relação a autenticação e a integridade de um documento ou mensagem eletrônica. É com certeza, um modelo mais adequado em comparação ao uso de usuário e senha, mesmo que o titular do certificado tenha que gerenciar alguns "riscos" remanescentes.

Apesar da longa crise política iniciada com a instauração da CPI dos Correios em 2005, seria muito importante que a tramitação do PL 7.316 parado na CCJC desde dezembro do ano passado, fosse retomada. Infelizmente, outras CPIs (Mensalão, Bingos, Sanguessugas) foram criadas e, ao investigar simultaneamente parlamentares, políticos, funcionários públicos, drenam grande parte da força produtiva tanto da Câmara quanto do Senado.

Aliando esses fatores a um ano eleitoral, com interesses muitas vezes voltados exclusivamente à reeleição, temos como conseqüência uma produtividade extremamente

baixa e um verdadeiro clima de “paralisia”. Acontece que o mundo não está parado e muitos países já consolidaram as suas normas jurídicas para atender às necessidades da Sociedade da Informação que estamos vivenciando hoje.

No Brasil, há a necessidade de reformulação do Processo Legislativo e atualização de muitas de nossas leis. Questões de grande impacto na sociedade e controversas, como os diversos aspectos do comércio eletrônico e a validade jurídica das assinaturas digitais, devem ser discutidas com mais agilidade e efetivamente regulamentadas. Caso isso não ocorra, corremos o risco de ficar à margem de um mercado globalizado, que movimenta bilhões de dólares em comércio eletrônico e ainda é possível que tenhamos que cumprir leis impostas por países que já consolidaram os seus institutos jurídicos.

Hoje, a popularização da certificação digital no Brasil, depende basicamente de três fatores: a disseminação dos conceitos básicos e da tecnologia de certificação digital para os potenciais usuários; a redução dos custos de sua utilização e a confiança adquirida nas entidades certificadoras pelo usuário final. Esse último fator não pode ser imposto, tem que ser adquirido e isso depende tanto da implementação tecnológica disponibilizada pelas entidades certificadoras, como da existência de uma legislação justa e aplicável na prática.

10. BIBLIOGRAFIA

[1] CERT. Tentativas de fraude pela Internet crescem 579% - CGI.br. Acessado em 20/08/2006 em http://www.cgi.br/releases/2006/rl-2006-01.pdf.

[2] LIVRO VERDE PARA A SOCIEDADE DA INFORMAÇÃO EM PORTUGAL. Missão para a Sociedade da Informação – Ministério da Ciência e da Tecnologia, p.102, Lisboa, 1997.

[3] TUCCI, R.L. Curso de Direito Processual Civil, vol. II, Ed. Saraiva, Rio de Janeiro,1989.

[4] FERREIRA, A.B.H. Novo Dicionário Aurélio da Língua Portuguesa – Nova Fronteira, Rio de Janeiro, 2004.

[5] ZAGAMI, Raimondo. Firme Digitali, Crittografia e Validità del Documento Elettronico. In: O Mercosul e a documentação eletrônica. Acessado em 07/05/2006 em http://www.advogado.com/zip/mercosul.htm.

[6] PAPEL. Enciclopédia Britannica online. Acessado em 28/05/2006 em http://www. Britannica.com/eb/article-9058327.

[7] SANTOS, M.A. Primeiras Linhas de Direito Processual Civil. vol. II, São Paulo, 1997.

[8] MARCACINI, A.T.R. Documento eletrônico como meio de prova. Acessado em 01/02/2006 em http://advogado.com/internet/zip/tavares.htm.

[9] TRUJILLO, E. O Mercosul e a documentação eletrônica. Acessado em 01/04/2006 em http://www.advogado.com/zip/mercosul.htm.

[10] HOUAISS, A. Dicionário Eletrônico Houaiss da Língua Portuguesa, v1.0 – Instituto Antônio Houaiss, 2004.

[11] THEODORO JR., H. Curso de direito processual civil, vol. I, Rio de Janeiro, 1996.

[12] FERREIRA, P.R.G. Documento eletrônico e sua validade em face do novo código civil. In: Questões de direito civil e o novo código – Ministério Público do Estado de São Paulo, São Paulo, 2004.

[13] GIANNANTONIO, E. Manuale di Diritto dell'Informatica. In: O Mercosul e a documentação eletrônica. Acessado em 21/05/2006 em http://www.advogado.com /zip/mercosul.htm.

[14] MARCACINI, A.T.R. Direito e Informática: uma abordagem jurídica sobre criptografia, Rio de Janeiro, 2002.

[15] FERREIRA, A.A.M.B. Sistemas tecnológicos e o poder judiciário. Acessado em 18/05/2006 em http://www.justicasempapel.org.br.

[16] SANTOLIM, C.V.M. Formação e eficácia probatória dos contratos por computador. São Paulo, Saraiva, 1995.

[17] MARQUES. A.T.G.L. A prova documental na Internet: validade e eficácia do documento eletrônico. Editora Juruá, Curitiba, 2005.

[18] BIOMETRICS CONSORTIUM. Introduction to Biometrics. The Biometrics Consortium. Acessado em 04/07/2006 em http://www.biometrics.org/intro.htm.

[19] DIFFIE, W.; HELLMAN, M. New Directions in Cryptography. IEEE Transactions on Information Theory, v. IT-22, nº 6, 1976, p. 644-654.

[20] RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, v21, nº 2, 1978.

[21] DA CUNHA, A. G. Dicionário etimológico Nova Fronteira. Nova Fronteira, Rio de Janeiro, 1982.

[22] CRIPTOGRAFIA. Enciclopédia Barsa. Cia Melhoramentos de São Paulo, v. 4, 1967.

[23] KAHN, D. The Codebreakers. Mcmillan, 1967. In: ELLISON, C. Cryptography timeline. Acessado em 13/06/2006 em http://world.std.com/~cme/html/timeline.html.

[24] BONAVOGLIA, P.; SAVARD, J.; TKOTZ, V. Cifras hebraicas. Acessado em 13/06/2006 em http://www.numaboa.com.br/criptologia/cifras/substituicao/hebreu.php.

[25] STALLINGS, W. Cryptography and Network Security – Principles and Practice. Prentice Hall, 3rd Ed., 2003.

[26] NIST. Announcing request for candidate algorithm nominations for the advanced encryption standard (AES). Acessado em 13/06/2006 em http://csrc.nist.gov/CryptoToolkit/aes/pre-round1/aes_9709.htm

[27] STEWART, W. Public Key Cryptography (PKC) History. Acessado em 24/06/2006 em http://www.livinginternet.com/i/is_crypt_pkc_inv.htm.

[28] INFINITY. The Feasibility of Breaking PGP. Acessado em 24/06/2006 em http://axion.physics.ubc.ca/pgp-attack.html.

[29] FERGUSON, N.; SCHNEIER, B. Practical Cryptography. Wiley Publishing, Inc., 2003.

[30] SCHNEIER, B. Secrets and Lies: Digital Security in a Networked World. Wiley Publishing, 2004.

[31] SCHNEIER, B. Factoring in Public-Key's Future. Acessado em 24/06/2006 em http://www.byte.com/art/9510/sec7/art5.htm.

[32] NECHVATAL, J. Public Key Cryptography. In SIMMONS, G. Contemporary

Cryptology: The Science of Information Integrity. IEEE Press, 1992.

[33] BOER, B.; BOSSELAERS, A. An Attack on the Last Two Rounds of MD4. Acessado em 26/06/2006 em http://citeseer.ist.psu.edu/denboer91attack.html.

[34] RIVEST, R. The MD5 Message-Digest Algorithm. Acessado em 26/06/2006 em http://theory.lcs.mit.edu/~rivest/Rivest-MD5.txt.

[35] Dobbertin, H. *Cryptanalysis of MD5*. EuroCrypt, Espanha, 1996.

[36] CHABAUD, F. JOUX, A. Differential Collisions in SHA-0. Advances in Cryptology - CRYPTO'98. Santa Barbara, USA, 1998.

[37] FIPS 180-2. Secure Hash Standard. Acessado em 26/06/2006 em http://csrc.nist.gov /publications/fips/fips180-2/fips180-2.pdf.

[38] RIJMEN, V.. BARRETO, P.S.L. The WHIRLPOOL Hash Function. Acessado em 27/06/2006 em http://paginas.terra.com.br/informatica/paulobarreto/WhirlpoolPage .html.

[39] ITI FAQ. O que é um Certificado Digital. Acessado em 12/07/2006 em http://www.iti.br/twiki/bin/view/Main/FaQ2003Jun24K.

[40] BURNETT, S.; PAINE, S. Criptografia e Segurança: O Guia Oficial RSA.Rio de Janeiro, Campus, 2002.

[41] CERTISIGN FAQ. ICP-Brasil. Acessado em 10/07/2006 em http://www. certisign.com.br/suporte/central_faqs/icpbrasil/icp.jsp

[42] VOLPI, M. M. Assinatura digital: Aspectos técnicos, práticos e legais. Rio de Janeiro, Axcel, 2001.

[43] ICP Brasil. Infra-estrutura de Chaves Públicas Brasileira. Acessado em 17/06/2006 em http://www.icpbrasil.gov.br.

[44] MP2.200-2. Medida Provisória 2.200-2. Acessado em 05/05/2006 em http://www .iti.gov.br/medidaprovisoria/medida_provis_ria_2_200_2_d.pdf.

[45] CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO. ICP Brasil. Acessado em 24/06/2006 em http://www.iconenet.com.br/cd/cd_guia.pdf

[46] ITI. Certificação Digital – Entenda e Utilize. Acessado em 24/06/2006 em http://iti.br/twiki/pub/Main/Cartilhas/CertificacaoDigital.pdf

[47] ICP-BRASIL. Requisitos mínimos para as políticas de certificado na ICP-Brasil, Resolução nº 41, de 18 de abril de 2006. Acessado em 10/07/2006 em http://www.iti.gov.br/resolucoes/resolu__o_41_de_18_04_2006.pdf.

[48] UTAH. Utah Digital Signature Act. Acessado em 06/05/2006 em http://www. rules.utah.gov/publicat/code/r154/r154-010.htm.

[49] UNCITRAL. Lei modelo da UNCITRAL sobre comércio eletrônico. Acessado em 12/07/2006 em http://www.dct.mre.gov.br/e-commerce/seminario_e-commerce_ lei.htm.

[50] CALIFORNIA. California Digital Signature Regulations. Acessado em 06/05/2006 em http://www.ss.ca.gov/digsig/regulations.htm.

[51] ILLINOIS. Public Act 90-0759. Acessado em 06/05/2006 em http://www. findlaw.com/bills/ildigital.html

[52] GEORGIA. Electronic Records and Signature Act. Acessado em 07/05/2006 em http://gsulaw.gsu.edu/gsuecp/Act/Act.htm.

[53] EUA. Electronic Signatures in Global and National Commerce Act, 2000. Acessado em 07/07/2006 em http://www.cbeji.com.br/br/downloads/secao/USDigitalLaw.pdf.

[54] ALEMANHA. Act on Digital Signature (Gesetz zur digitalen Signatur) Acessado em 07/05/2006 em http://www.iuscomp.org/gla/statutes/SiG.htm.

[55] ITALIA. Decreto del Presidente della Repubblica 10 novembre 1997, nº 513. Acessado em 08/05/2006 em http://www.interlex.it/testi/dpr51397.htm.

[56] INGLATERRA. Electronic Communications Act, 2000. Acessado em 08/05/2006 em http://www.opsi.gov.uk/acts/acts2000/20000007.htm.

[57] FRANÇA. Loi n° 2000-230 de 2000. Acessado em 08/05/2006 em http://www .legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSX9900020L.

[58] PORTUGAL. Decreto-Lei n.º 290-D, 1999. Acessado em 08/05/2006 em http://www.pj.pt/htm/legislacao/dr_informatica/DL290_D_99.htm.

[59] DIRETIVA EUROPÉIA. Diretiva 1999/93/EC. Acessado em 10/04/2006 em http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en001200 20.pdf.

[60] CHILE. Decreto Supremo n. 81 de 1999. Acessado em 09/05/2006 em http://rechtsinformatik.jura.uni-sb.de/cbl/statutes/Chile81.html.

[61] COLÔMBIA. Lei 527 de 1999. Acessado em 09/05/2006 em http://www.secretaria senado.gov.co/leyes /L0527_99.htm.

[62] ARGENTINA. Decreto nº 427 de 1998. Acessado em 09/05/2006 em http://www .informatica-juridica.com/anexos/anexo193.asp.

[63] CÂMARA DOS DEPUTADOS. Processo Legislativo. Acessado em 14/07/2006 em http://www2.camara.gov.br/processolegislativo/processoLegislativo.pdf.

[64] FLUXO LEGISLATIVO. Fluxo simplificado do Processo Legislativo (adaptado). Acessado em 28/07/2006 em http://www2.camara.gov.br/processolegislativo.

[65] EMENDA. Índice Fundamental do Direito – Emenda Constitucional. Acessado em

12/07/2006 em http://www.dji.com.br/constitucional/emenda_a_constituicao.htm.

[66] QUEIROZ, A. F. Direito Constitucional. IEPC, 2006.

[67] LEI COMPLEMENTAR. Índice Fundamental do Direito – Lei Complementar. Acessado em 12/07/2006 em http://www.dji.com.br/constitucional/leis_complementares.htm

[68] LEI ORDINÁRIA. Índice Fundamental do Direito – Lei Ordinária. Acessado em 12/07/2006 em http://www.dji.com.br/constitucional/lei_ordinaria.htm.

[69] LEI DELEGADA. Índice Fundamental do Direito – Lei Delegada. Acessado em 12/07/2006 em http://www.dji.com.br/constitucional/lei_delegada.htm.

[70] EXECUTIVO. Emenda Constitucional nº 32 de 2001. Acessado em 12/07/2006 em http://www2.camara.gov.br/internet/legislacao/legin.html/textos/visualizarTexto.html?ideNorma=395730&seqTexto=1.

[71] LENZA, PEDRO. Direito Constitucional Esquematizado, São Paulo, 2005.

[72] RESOLUÇÃO. Conceito de Resolução. Acessado em 07/07/2006 em http://www.al.ap.gov.br/pleg1a.htm.

[73] DECRETO. Índice Fundamental do Direito – Decreto. Acessado em 17/07/2006 em http://www.dji.com.br/constitucional/decreto.htm.

[74] GOVERNO. Portal do Governo Eletrônico. Acessado em 25/07/2006 em http://www.governoeletronico.gov.br/governoeletronico.

[75] COMITÊ GESTOR ICP-BRASIL. Estrutura Normativa da ICP-Brasil v. 1.0. Acessado em 29/07/2006 em http://www.iti.gov.br/impressao/estrutura_normativa/estrutura_normativa.pdf.

[76] MDIC. Comitê Executivo de Comércio Eletrônico. Acessado em 25/07/2006 em http://ce.mdic.gov.br

[77] ASCOM MDIC. Primeira reunião Comitê Executivo de Comércio Eletrônico. Acessado em 28/07/2006 em http://www.desenvolvimento.gov.br/sitio/ascom/noticias/noticia.php?cd_noticia=5802.

[78] RSA LABORATORIES. Public Key Issues. Acessado em 02/06/2006 em http://www. rsasecurity.com/rsalabs/node.asp?id=2273

[79] SECURITY Warnings. Man in the middle attack. Acessado em 03/06/2006 em http://www.securitywarnings.com/encyclopedia/?id=13

[80] ALLEMAND, M.. Interoperabilidade – condição para o sucesso dos serviços de uma ICP. I Forum de Segurança, Privacidade e Certificação Digital. Brasília, 2003.

[81] ALTERMAN, P. PKI at the Crossroads. Acessado em 14/08/2006 em http://www.fcw .com/fcw/articles/2002/0624/tec-pki-06-24-02.asp.

[82] MERKLE, R.; HELLMAN, M. Hiding Information and Signatures in Trapdoor Knapsacks, IEEE Trans. Information Theory, p525–530, Setembro 1978.

[83] SHAMIR, A. A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem. Acessado em 02/06/2006 em http://dsns.csie.nctu.edu.tw/research /crypto/HTML/PDF/C82/279.pdf.

[84] NIST. Digital Signature Standard. DSA, RSA, and ECDSA algorithms. Acessado em 08/08/2006 em http://csrc.nist.gov/cryptval/dss.htm.

[85] WIKEPEDIA 3DES. 3DES. Acessado em 10/08/2006 em http://en.wikipedia.org /wiki/3DES.

[86] WIKEPEDIA IDEA. International Data Encryption Algorithm. Acessado em 10/08/ 2006 em http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm.

[87] WIKEPEDIA SAFER+. Secure And Fast Encryption Routine. Acessado em 10/08/ 2006 em http://en.wikipedia.org/wiki/SAFER_plus.

[88] CERTFORUM. 4º Forum de Certificação Digital - http://www.certforum.com.br. Brasília, 2006.

[89] ITI. ITI entrega códigos-fonte para a sociedade. Acessado em 14/08/2006 em http://www.iti.br/twiki/bin/view/Main/PressRelease2005Jun28A.

[90] FGV, EAESP. 17ª pesquisa anual "Mercado Brasileiro de Informática e Uso nas Empresas". Rio de Janeiro, 2006.

[91] FREITAS, A.N.; BASSANI, H.F. Risco no uso de certificados digitais de chave pública – Análise de vulnerabilidades nos navegadores com SSL. Acessado em 14/08/2006 em http://www.cic.unb.br/docentes/pedro/trabs/riscocert.htm.

[92] MICROSOFT. Definindo softwares mal intencionados. Acessado em 14/08/2006 em http://www.technetbrasil.com.br/Artigos/Seguranca/SoftMalIntenc.aspx.

[93] GAIGER FERREIRA, P.R. Documento eletrônico e sua validade em face do novo código civil. In: Questões de Direito Civil e o novo Código. Ministério Público do Estado de São Paulo. São Paulo, 2004.

[94] MARTINS FILHO, I. G. Agravo de Instrumento em Recurso Ordinário 76787/2003-900-02-00.4. Diário Oficial da União de 13/06/2003.

[95] REZENDE, A.D. Privacidade e Riscos num mundo de chaves públicas. I Fórum sobre Segurança, Privacidade e Certificação Digital, Brasília, 2003.

[96] CARNUT. M. Certificados Digitais Pseudônimos: Identificação Segura e Privacidade são Compatíveis. I Fórum sobre Segurança, Privacidade e Certificação Digital, Brasí-lia, 2003.

[97] MENKE, F. Assinatura Eletrônica no Direito Brasileiro. Editora Revista dos Tribunais, São Paulo, 2005.

[98] SCHENEIER, B. Segurança.com – Segredos e mentiras sobre a proteção na vida digital. Editora Campus, 2001.

[99] PEC72. Proposta de Emenda à Constituição 72 de 2005. Acessado em 19/08/2006 em http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=313951.

[100] E-CAC. Instrução Normativa SRF n° 580, de 12 de dezembro de 2005. Acessado em 19/08/2006 em http://www.receita.fazenda.gov.br/Legislacao/Ins/2005/in5802005.htm.

[101] SPB. Confiabilidade no trânsito de mensagens do SPB. Acessado em 19/08/2006 em http://www.certisign.com.br/certinews/banconoticias/2006/julho/julho_04_Confiabilidade_no_transito.jsp.

[102] SISPROUNI. O Sistema PROUNI. Acessado em 19/08/2006 em em http://prouni-inscricao.mec.gov.br/prouni/Oprograma.shtm.

[103] FINEP. Programa de financiamento para micro e pequena empresa, FINEP Juro Zero. Acessado em 19/08/2006 em http://www.certisign.com.br/solucoes/jurozero.

[104] ITI. STF adota certificação digital para servidores. Acessado em 19/08/2006 em http://www.iti.br/twiki/bin/view/Main/PressRelease2006Jun28B.

[105] OAB. Pedido de Providências da OAB ao CNJ para revisão da IN 28/2005. Acessado em 19/08/2006 em http://www.ibdi.org.br/index.php?secao=&id_noticia=513&acao=lendo.

11. ANEXO I – LEGISLAÇÃO

PROJETO DE LEI DA CÂMARA Nº 2.644 DE 1996

Autor: Dep. Jovair Arantes

Dispõe sobre a elaboração, o arquivamento e o uso de documentos eletrônicos.

O Congresso Nacional decreta:

Art. 1º Considera-se documento eletrônico, para os efeitos desta Lei, todo documento, público ou particular, originado por processamento eletrônico de dados e armazenado em meio magnético, optomagnético, eletrônico ou similar.

Art. 2º Considera-se original o documento eletrônico autenticado por assinatura eletrônica, processado segundo procedimentos que assegurem sua autenticidade e armazenado de modo a preservar sua integridade.

Art. 3º No caso de transações que gerem grandes volumes de registros ou informações complexas, é admissível a aceitação de um sumário da operação para sua comprovação, desde que os registros detalhados estejam disponíveis a qualquer momento.

Art. 4º É cópia fiel a impressão em papel dos dados contidos em documento eletrônico autenticado, desde que obtida por meios que assegurem sua fidedignidade aos dados originais.

Art. 5º É obrigação do administrador de recursos computacionais que produz, armazena, processa ou transmite documento eletrônico:

I - assegurar proteção contra acesso, uso, alteração, reprodução ou destruição indevida dos documentos;
II - prover métodos e processos racionais que facilitem a busca de documentos;
III - manter registro de todos os procedimentos efetuados nos documentos para fins de auditoria;
IV - prever procedimentos de segurança a serem adotados em caso de acidentes que possam danificar, destruir ou impossibilitar o acesso aos dados armazenados ou em processamento.

Art. 6º Constitui crime:

I - utilizar ou reproduzir indevidamente documento eletrônico;
Pena - reclusão de 1 (um) a 2 (dois) anos e multa;
II - modificar ou destruir documento eletrônico de outrem;
Pena - reclusão de 2 (dois) anos a 5 (cinco) anos e multa;
III - interferir indevidamente no funcionamento do computador ou rede de computadores provocando a modificação ou destruição de documento eletrônico;
Pena - reclusão de 2 (dois) a 6 (seis) anos e multa;
IV - Impossibilitar ou dificultar o legítimo acesso a documento eletrônico;
Pena - detenção de 1 (um) a 3 (três) anos e multa;
V - Deixar o administrador de recursos computacionais de armazenar documento eletrônico:

a) em equipamento que não disponha de registro dos procedimentos efetuados;

b) sem manter procedimentos de segurança para o caso de acidente;
Pena - detenção de 1 (um) a 2 (dois) anos e multa.

Art. 7º Esta lei entra em vigor na data de sua publicação.

Art. 8º Revogam-se as disposições em contrário.

PROJETO DE LEI DO SENADO N° 3.173 DE 26 DE MAIO DE 1997

Autor: Sen. Sebastião Rocha

Dispõe sobre os documentos produzidos e os arquivados em meios eletrônicos e dá outras providências.

O Congresso Nacional decreta:

Art. 1° É autorizado em todo o território nacional o arquivamento em meio eletrônico de informações, dados, imagens e quaisquer outros documentos que constituam o acervo documental das empresas privadas e órgãos e entidades da Administração Pública Federal, Estadual e Municipal direta e indireta, das fundações instituídas ou mantidas pelo Poder Público e demais organizações sobre controle direto ou indireto da União e do Distrito Federal, garantida a integridade do acervo.

§ 1 O arquivamento de documentos em meio eletrônico dependerá de disciplinamento próprio nas empresas privadas e órgãos de entidades da Administração Pública Federal, Estadual e Municipal direta e indireta, das fundações instituídas ou mantidas pelo Poder Público e demais organizações sobre controle direto ou indireto da União e do Distrito Federal, observando o que determina o decreto regulamentador específico.

§ 2° Os registros originais, independentemente de seus suportes ou meio onde foram gerados, após serem arquivados eletronicamente, poderão, a critério da autoridade competente, ser eliminados ou transferidos para outro suporte e local, observada a legislação pertinente.

§ 3° Para os efeitos de preservação da integridade dos documentos, o meio eletrônico utilizado, qualquer que seja sua forma ou natureza, deverá garantir a autenticidade, a indelibilidade e a confidencialidade dos documentos, protegendo-os contra todo o acesso, uso, alteração de conteúdo ou qualidade, reprodução, e destruição não autorizadas.

§ 4° Terão valor probante, em juízo ou fora dele, as reproduções obtidas do sistema de arquivamento eletrônico, desde que sejam perfeitamente legíveis e fiéis aos respectivos registros originais e atendam ao decreto regulamentador especifico.

Art. 2° As unidades da Administração Pública direta e indireta, as fundações e organizações sob controle direto ou indireto da União, Distrito Federal, Estados e Municípios e as empresas privadas para se utilizarem de sistema de arquivamento eletrônico deverão manter procedimentos voltados à gestão de seus documentos, conforme a sua conveniência e preceituado em Lei.

§ 1° Os documentos arquivados eletronicamente, utilizarão obrigatoriamente um sistema de indexação e obedecerão a um processo previamente documentado e aprovado pela autoridade competente.

§ 2° O sistema de arquivamento eletrônico deverá propiciar uma rápida e eficiente localização dos documentos, bem como permitir a verificação da fidelidade ao processo previamente definido e aprovado pela autoridade competente.

Art. 3° É assegurado o acesso aos documentos dos órgãos públicos e instituições de caráter público, produzidos e os arquivados em meio eletrônico, ressalvados aqueles considerados como segredo de justiça e sigilosos, na forma da legislação em vigor.

Art. 4° As dúvidas ou questionamentos sobre as reproduções obtidas de sistemas de arquivamento eletrônico deverão ser dirimidas a partir da documentação do processo aprovado pela autoridade competente e respectivos originais.

Art. 5° Ficarão sujeito a responsabilidade penal, civil e administrativa, de acordo com a Legislação em vigor, aquele que desfigurar ou destruir documentos de valor permanente ou considerado como de interesse público e social arquivados, produzidos ou reproduzidos na forma prevista nesta Lei.

Art. 6° Esta Lei entra em vigor na data de sua publicação.

Art. 7° Revogam-se as disposições em contrário.

PROJETO DE LEI DA CÂMARA Nº 4.734 DE 12 DE AGOSTO DE 1998

Autor: Dep. Paulo Lima

Dispõe sobre a informatização, no âmbito da Lei nº 6.015 de 31 de dezembro de 1973 – Lei de Registros Públicos – da escrituração cartorária através de discos ópticos e optomagnéticos ou em outros meios reconhecidos como legais, sem prejuízo dos métodos atualmente empregados.

O Congresso Nacional decreta:

Art. 1º Acrescente-se o seguinte art. 7ºA, à Lei nº 6.015, de 31 de dezembro de 1973 – Lei sobre os Registros Públicos:

"Art. 7ºA Sem prejuízo dos métodos atualmente utilizados e de outros que vierem a ser estabelecidos em lei, na escrituração a que se refere esta lei poderá ser empregada a informatização com a utilização de discos ópticos e optomagnéticos, observadas as disposições do capítulo V deste Título.

Art. 2º Esta lei entra em vigor na data de sua publicação.

EXCERTO DA LEI Nº 6.015, DE 31 DE DEZEMBRO DE 1973

CAPÍTULO V

Da Conservação

Art. 22. Os livros de registro, bem como as fichas que os substituam, somente sairão do respectivo cartório mediante autorização judicial.

Art. 23. Todas as diligências judiciais e extrajudiciais que exigirem a apresentação de qualquer livro, ficha substitutiva de livro ou documento, efetuar-se-ão no próprio cartório.

Art. 24. Os oficiais devem manter, em segurança, permanentemente, os livros e documentos e respondem pela sua ordem e conservação.

Art. 25. Os papéis referentes ao serviço do registro serão arquivados em cartório mediante a utilização de processos racionais que facilitem as buscas, facultada a utilização de microfilmagem e de outros meios de reprodução autorizados em lei.

Art. 26. Os livros e papéis pertencentes ao arquivo do cartório ali permanecerão indefinidamente.

Art. 27. Quando a lei criar novo cartório, e enquanto este não for instalado, os registros continuarão a ser feitos no cartório que sofreu o desmembramento, não sendo necessário repeti-los no novo ofício.

Parágrafo único. O arquivo do antigo cartório continuará a pertencer-lhe.

DECRETO Nº 2.954 DE 29 DE JANEIRO DE 1999
(Revogado pelo DECRETO Nº 4.176, DE 28 DE MARÇO DE 2002)
Autor: Poder Executivo

Estabelece regras para a redação de atos normativos de competência dos órgãos do Poder Executivo.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição, e tendo em vista o disposto na Lei Complementar nº 95, de 26 de fevereiro de 1998, e Considerando a necessidade do controle de juridicidade e legitimidade dos atos normativos, assim como a uniformização dos atos e procedimentos administrativos,

DECRETA:

CAPÍTULO I - DA ELABORAÇÃO DOS ATOS NORMATIVOS

Art. 1º. Os órgãos e as entidades da Administração Pública Federal observarão as normas e diretrizes constantes deste Decreto e as do Manual de Redação da Presidência da República na elaboração dos seguintes atos a serem encaminhados à Casa Civil da Presidência da República, e, no que couber, aos demais atos de regulamentação expedidos por órgãos do Poder Executivo:

Art. 57-A. A partir de 1o de janeiro de 2001, os documentos a que se refere este Decreto somente serão recebidos, na Casa Civil da Presidência da República, por meio eletrônico.-(Artigo incluído pelo Decreto nº 3.585, de 05/09/2000)

OBS: O texto deste decreto é de volume razoável e para tanto foram expostos somente os artigos relevantes ao tema do presente trabalho para fins de clareza e concisão.

PROJETO DE LEI DA CÂMARA Nº 1.483 DE 12 DE AGOSTO 1999
Autor: Dep. Hélio de Oliveira Santos

Institui a fatura eletrônica e a assinatura digital nas transações de "comércio" eletrônico.

Art. 1º Fica instituída a fatura eletrônica, assim como a assinatura digital, nas transações comerciais eletrônicas realizadas em todo o território nacional.

Art. 2º A assinatura digital terá sua autenticação e reconhecimento certificado por órgão público que será regulamentado para este fim.

Parágrafo Único. Toda documentação eletrônica, bem como o cadastro de assinaturas digitais, deverão estar com seus registros disponíveis para avaliação e fiscalização dos órgãos federais responsáveis.

PROJETO DE LEI DA CÂMARA Nº 1.532 DE 19 DE AGOSTO DE 1999

Autor: Dep. Angela Guadagnin

Dispõe sobre a elaboração e arquivamento de documentos em meios eletromagnéticos

O Congresso Nacional decreta:

Art. 1º São válidos e eficazes, para qualquer efeito, os documentos públicos e particulares elaborados ou arquivados em qualquer meio eletromagnético ou equivalente que preserve a integridade dos documentos.

Parágrafo Único – Para os efeitos de preservação da integridade de documentos, o meio eletrônico utilizado, qualquer que seja sua forma ou natureza, deverá garantir a segurança, a autenticidade, a nitidez, a indelebilidade e a confidencialidade dos documentos, protegendo-os contra todo acesso, uso, alteração, reprodução e destruição não autorizados.

Art. 2º Para os fins desta Lei e de sua regulamentação, entende-se por documento qualquer instrumento através do qual se formalizam ou registram atos jurídicos, em qualquer de suas modalidades, sejam eles de natureza civil, comercial, administrativa, tributária, trabalhista, processual ou outra.

Art. 3º Observadas as disposições desta Lei e de sua regulamentação, a reprodução, inclusive em papel, a partir do meio eletrônico em que o documento é elaborado ou arquivado, é considerada documento original para todos os efeitos legais.

§1º - Será vedada a exigência de exibição em papel dos documentos nesta forma originalmente elaborados, quando estiverem arquivados em meio eletrônico, nos termos desta lei.
§2º - Em decorrência do disposto no parágrafo anterior, será facultada a destruição dos documentos originais em papel cujo arquivamento esteja sendo feito em meio eletrônico, nos termos desta Lei, ressalvados os documentos de valor histórico, cuja preservação deverá observar a legislação pertinente.

Art. 4º Para assegurar a integridade dos documentos elaborados ou arquivados na forma prevista nesta Lei, serão adotados, dentre outros, os mecanismos tecnológicos disponíveis de assinatura eletrônica e de códigos personalizados para o acesso, reprodução e transmissão de documentos, bem como de métodos eficazes de preservação de documentos em situações de emergência, tais como incêndios, inundações, greves e outras que possam colocar em risco os sistemas computacionais utilizados para os fins aqui previstos.

Parágrafo Único – Em qualquer caso, na utilização de meio eletrônico na forma e para os fins previstos nesta Lei, deverão ser adotados métodos e processos racionais que facilitem a busca de documentos, e que garantam trilhas de auditoria.

Art. 5º Quando se tratar de registros públicos, o meio eletrônico utilizado deverá garantir os requisitos de arquivamento e preservação permanentes dos documentos, para os efeitos do disposto na legislação pertinente.
Parágrafo Único – Nos demais casos, e desde que decorridos os respectivos prazos de decadência ou prescrição e mediante a competente autorização, os documentos poderão ser destruídos por qualquer meio que assegure sua desintegração.

Art. 6º Competirá a Associação Brasileira de Normas Técnicas ABNT emitir norma fixando os requisitos técnicos a serem observados para os efeitos desta Lei.

Art. 7º A infração a qualquer das disposições desta Lei e de sua regulamentação sujeitará o infrator às penalidades previstas na legislação brasileira.

Art. 8º Esta Lei entra em vigor na data de sua publicação.

Art. 9º Revogam-se as disposições em contrário.

PROJETO DE LEI DA CÂMARA Nº 1.589 DE 31 DE AGOSTO DE 1999

Autor: Dep. Luciano Pizzatto e outros (OAB)

Dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências.

(Apense-se ao projeto de lei nº 1.483, de 1999.)

O Congresso Nacional decreta:

Título I - Definições Gerais

Capítulo I – Do âmbito de aplicação

Art. 1º - A presente lei regula o comércio eletrônico, a validade e o valor probante dos documentos eletrônicos, bem como a assinatura digital.

Capítulo II – Dos princípios gerais

Art. 2º - A interpretação da presente lei deve considerar o contexto internacional do comércio eletrônico, o dinâmico progresso dos instrumentos tecnológicos, e a boa-fé das relações comerciais. Parágrafo único - As questões relativas a matérias regidas pela presente lei, e que não estejam nela expressamente previstas, serão dirimidas de conformidade com os princípios gerais que dela decorrem.

Título II - Comércio Eletrônico

Capítulo I – Da desnecessidade de autorização prévia

Art. 3º - O simples fato de ser realizada por meio eletrônico não sujeitará a oferta de bens, serviços e informações a qualquer tipo de autorização prévia.

Capítulo II – Das informações prévias

Art. 4º - A oferta de contratação eletrônica deve conter claras e inequívocas informações sobre: a) nome do ofertante, e o número de sua inscrição no cadastro geral do Ministério da Fazenda, e ainda, em se tratando de serviço sujeito a regime de profissão regulamentada, o número de inscrição no órgão fiscalizador ou regulamentador; b) endereço físico do estabelecimento; c) identificação e endereço físico do armazenador; d) meio pelo qual é possível contatar o ofertante, inclusive correio eletrônico; e) o arquivamento do contrato eletrônico, pelo ofertante; f) instruções para arquivamento do contrato eletrônico, pelo aceitante, bem como para sua recuperação, em caso de necessidade; e g) os sistemas de segurança empregados na operação.

Capítulo III – Das informações privadas do destinatário

Art. 5º - O ofertante somente poderá solicitar do destinatário informações de caráter privado necessárias à efetivação do negócio oferecido, devendo mantê-las em sigilo, salvo se prévia e expressamente autorizado a divulgá-las ou cedê-las pelo respectivo titular. § 1º - A autorização de que trata o caput deste artigo constará em destaque, não podendo estar vinculada à aceitação do negócio. § 2º - Responde por perdas e danos o ofertante que solicitar, divulgar ou ceder informações em violação ao disposto neste artigo.

Capítulo IV – Da contratação eletrônica

Art. 6º - A oferta pública de bens, serviços ou informações à distância deve ser realizada em ambiente seguro, devidamente certificado.

Art. 7º - Os sistemas eletrônicos do ofertante deverão transmitir uma resposta eletrônica automática, transcrevendo a mensagem transmitida anteriormente pelo destinatário, e confirmando seu recebimento.

Art. 8º - O envio de oferta por mensagem eletrônica, sem prévio consentimento dos destinatários, deverá permitir a estes identificá-la como tal, sem que seja necessário tomarem conhecimento de seu conteúdo.

Capítulo V – Dos intermediários

Art. 9º - O intermediário que forneça serviços de conexão ou de transmissão de informações, ao ofertante ou ao adquirente, não será responsável pelo conteúdo das informações transmitidas.

Art. 10 - O intermediário que forneça ao ofertante serviços de armazenamento de arquivos e de sistemas necessários para operacionalizar a oferta eletrônica de bens, serviços ou informações, não será responsável pelo seu conteúdo, salvo, em ação regressiva do ofertante, se: a) deixou de atualizar, ou os seus sistemas automatizados deixaram de atualizar, as informações objeto da oferta, tendo o ofertante tomado as medidas adequadas para efetivar as atualizações, conforme instruções do próprio armazenador; ou b) deixou de arquivar as informações, ou, tendo-as arquivado, foram elas destruídas ou modificadas, tendo o ofertante tomado as medidas adequadas para seu arquivamento, segundo parâmetros estabelecidos pelo armazenador.

Art. 11 - O intermediário, transmissor ou armazenador, não será obrigado a vigiar ou fiscalizar o conteúdo das informações transmitidas ou armazenadas. Parágrafo único – Responde civilmente por perdas e danos, e penalmente, por co-autoria do delito praticado, o armazenador de informações que, tendo conhecimento inequívoco de que a oferta de bens, serviços ou informações constitui crime ou contravenção penal, deixar de promover sua imediata suspensão, ou interrupção de acesso por destinatários, competindo-lhe notificar, eletronicamente ou não, o ofertante, da medida adotada.

Art. 12 - O intermediário deverá guardar sigilo sobre as informações transmitidas, bem como sobre as armazenadas, que não se destinem ao conhecimento público. Parágrafo único - Somente mediante ordem judicial poderá o intermediário dar acesso às informações acima referidas, sendo que as mesmas deverão ser mantidas, pelo respectivo juízo, em segredo de justiça.

Capítulo VI – Das normas de proteção e de defesa do consumidor

Art. 13 - Aplicam-se ao comércio eletrônico as normas de defesa e proteção do consumidor. § 1º - Os adquirentes de bens, de serviços e informações mediante contrato eletrônico poderão se utilizar da mesma via de comunicação adotada na contratação, para efetivar notificações e intimações extrajudiciais, a fim de exercerem direito consagrado nas normas de defesa do consumidor. § 2º - Deverão os ofertantes, no próprio espaço que serviu para oferecimento de bens, serviços e informações, disponibilizar área específica para fins do parágrafo anterior, de fácil identificação pelos consumidores, e que permita seu armazenamento, com data de transmissão, para fins de futura

comprovação. § 3º - O prazo para atendimento de notificação ou intimação de que trata o parágrafo primeiro começa a fluir da data em que a respectiva mensagem esteja disponível para acesso pelo fornecedor. § 4º - Os sistemas eletrônicos do ofertante deverão expedir uma resposta eletrônica automática, incluindo a mensagem do remetente, confirmando o recebimento de quaisquer intimações, notificações, ou correios eletrônicos dos consumidores.

Título III - Documentos Eletrônicos
Capítulo I - Da eficácia jurídica dos documentos eletrônicos

Art. 14 - Considera-se original o documento eletrônico assinado pelo seu autor mediante sistema criptográfico de chave pública. § 1º - Considera-se cópia o documento eletrônico resultante da digitalização de documento físico, bem como a materialização física de documento eletrônico original. § 2º - Presumem-se conformes ao original, as cópias mencionadas no parágrafo anterior, quando autenticadas pelo escrivão na forma dos arts. 33 e 34 desta lei. § 3º - A cópia não autenticada terá o mesmo valor probante do original, se a parte contra quem foi produzida não negar sua conformidade.

Art. 15 - As declarações constantes do documento eletrônico, digitalmente assinado, presumem-se verdadeiras em relação ao signatário, desde que a assinatura digital: a) seja única e exclusiva para o documento assinado; b) seja passível de verificação; c) seja gerada sob o exclusivo controle do signatário; d) esteja de tal modo ligada ao documento eletrônico que, em caso de posterior alteração deste, a assinatura seja invalidada; e e) não tenha sido gerada posteriormente à expiração, revogação ou suspensão das chaves.

Art. 16 - A certificação da chave pública, feita pelo tabelião na forma do Capítulo II do Título IV desta lei, faz presumir sua autenticidade.

Art.17 - A certificação de chave pública, feita por particular, prevista no Capítulo I do Título IV desta lei, é considerada uma declaração deste de que a chave pública certificada pertence ao titular indicado e não gera presunção de autenticidade perante terceiros. Parágrafo único - Caso a chave pública certificada não seja autêntica, o particular, que não exerça a função de certificação de chaves como atividade econômica principal, ou de modo relacionado à sua atividade principal, somente responderá perante terceiros pelos danos causados quando agir com dolo ou fraude.

Art. 18 - A autenticidade da chave pública poderá ser provada por todos os meios de direito, vedada a prova exclusivamente testemunhal.

Art. 19 - Presume-se verdadeira, entre os signatários, a data do documento eletrônico, sendo lícito, porém, a qualquer deles, provar o contrário por todos os meios de direito. § 1º - Após expirada ou revogada a chave de algum dos signatários, compete à parte a quem o documento beneficiar a prova de que a assinatura foi gerada anteriormente à expiração ou revogação. § 2º - Entre os signatários, para os fins do parágrafo anterior, ou em relação a terceiros, considerar-se-á datado o documento particular na data: I - em que foi registrado; II - da sua apresentação em repartição pública ou em juízo; III - do ato ou fato que estabeleça, de modo certo, a anterioridade da formação do documento e respectivas assinaturas.

Art. 20 - Aplicam-se ao documento eletrônico as demais disposições legais relativas à prova documental, que não colidam com as normas deste Título.

Capítulo II - Da falsidade dos documentos eletrônicos

Art. 21 - Considera-se falso o documento eletrônico quando assinado com chaves fraudulentamente geradas em nome de outrem.

Art. 22 - O juiz apreciará livremente a fé que deva merecer o documento eletrônico, quando demonstrado ser possível alterá-lo sem invalidar a assinatura, gerar uma assinatura eletrônica idêntica à do titular da chave privada, derivar a chave privada a partir da chave pública, ou pairar razoável dúvida sobre a segurança do sistema criptográfico utilizado para gerar a assinatura.

Art. 23 - Havendo impugnação do documento eletrônico, incumbe o ônus da prova: I - à parte que produziu o documento, quanto à autenticidade da chave pública e quanto à segurança do sistema criptográfico utilizado; II – à parte contrária à que produziu o documento, quando alegar apropriação e uso da chave privada por terceiro, ou revogação ou suspensão das chaves. Parágrafo único - Não sendo alegada questão técnica relevante, a ser dirimida por meio de perícia, poderá o juiz, ao apreciar a segurança do sistema criptográfico utilizado, valer-se de conhecimentos próprios, da experiência comum, ou de fatos notórios.

Título IV – Certificados Eletrônicos

Capítulo I – Dos certificados eletrônicos privados

Art. 24 - Os serviços prestados por entidades certificadoras privadas são de caráter comercial, essencialmente privados e não se confundem em seus efeitos com a atividade de certificação eletrônica por tabelião, prevista no Capítulo II deste Título.

Capítulo II – Dos certificados eletrônicos públicos

Seção I - Das certificações eletrônicas pelo tabelião

Art. 25 - O tabelião certificará a autenticidade de chaves públicas entregues pessoalmente pelo seu titular, devidamente identificado; o pedido de certificação será efetuado pelo requerente em ficha própria, em papel, por ele subscrita, onde constarão dados suficientes para identificação da chave pública, a ser arquivada em cartório. § 1º - O tabelião deverá entregar ao solicitante informações adequadas sobre o funcionamento das chaves pública e privada, sua validade e limitações, bem como sobre os procedimentos adequados para preservar a segurança das mesmas. § 2º - É defeso ao tabelião receber em depósito a chave privada, bem como solicitar informações pessoais do requerente, além das necessárias para desempenho de suas funções, devendo utilizá-las apenas para os propósitos da certificação.

Art. 26 – O certificado de autenticidade das chaves públicas deverá conter, no mínimo, as seguintes informações: I – identificação e assinatura digital do tabelião; II – data de emissão do certificado; III – identificação da chave pública e do seu titular, caso o certificado não seja diretamente apensado àquela; IV – elementos que permitam identificar o sistema criptografado utilizado; V – nome do titular e poder de representação de quem solicitou a certificação, no caso do titular ser pessoa jurídica. Parágrafo único – Na falta de informação sobre o prazo de validade do certificado, este será de 2 (dois) anos, contados da data de emissão.

Seção II – Da revogação de certificados eletrônicos

Art. 27 – O tabelião deverá revogar um certificado eletrônico: a) a pedido do titular da chave de assinatura ou de seu representante; b) de ofício ou por determinação do Poder Judiciário, caso se verifique que o certificado foi expedido baseado em informações falsas; e c) se tiver encerrado suas atividades, sem que tenha sido sucedido por outro tabelião. 1º - A revogação deve indicar a data a

partir da qual será aplicada. § 2º - Não se admite revogação retroativa, salvo nas hipóteses dos parágrafos 3º e 4º do art. 28.

Art. 28 – O titular das chaves é obrigado a adotar as medidas necessárias para manter a confidencialidade da chave privada, devendo revogá-la de pronto, em caso de comprometimento de sua segurança. § 1º - A revogação da chave pública certificada deverá ser feita perante o tabelião que emitiu o certificado; se a chave revogada contiver certificados de autenticidade de vários oficiais, a revogação poderá ser feita perante qualquer deles, ao qual competirá informar os demais, de imediato. § 2º - A revogação da chave pública somente poderá ser solicitada pelo seu titular ou por procurador expressamente autorizado. § 3º - Pairando dúvida sobre a legitimidade do requerente, ou não havendo meios de demonstrá-la em tempo hábil, o tabelião suspenderá provisoriamente, por até trinta dias, a eficácia da chave pública, notificando imediatamente o seu titular, podendo, para tanto, utilizar-se de mensagem eletrônica; revogada a chave dentro deste prazo, os efeitos da revogação retroagirão à data da suspensão. § 4º - Havendo mera dúvida quanto à segurança da chave privada, é lícito ao titular pedir a suspensão dos certificados por até trinta dias, aplicando-se o disposto na parte final do parágrafo anterior.

Art. 29 - O tabelião deverá manter serviço de informação, em tempo real e mediante acesso eletrônico remoto, sobre as chaves por ele certificadas, tornando-as acessíveis ao público, fazendo-se menção às que tenham sido revogadas.

Art. 30 – O tabelião somente poderá certificar chaves geradas por sistema ou programa de computador que tenha recebido parecer técnico favorável a respeito de sua segurança e confiabilidade, emitido pelo Ministério da Ciência e Tecnologia.

Seção III - Do encerramento das atividades de certificação

Art. 31 - Caso encerre as atividades de certificação eletrônica, o tabelião deverá assegurar que os certificados emitidos sejam transferidos para outro tabelião, ou sejam bloqueados.

Art. 32 – O tabelião deverá transferir as documentações referidas nos arts. 25 e 40 desta lei, ao tabelião que lhe suceder, ou, caso não haja sucessão, ao Poder Judiciário.

Seção IV – Da autenticação eletrônica

Art. 33 – A assinatura digital do tabelião, lançada em cópia eletrônica de documento físico original, tem o valor de autenticação.

Art. 34 – A autenticação de cópia física de documento eletrônico original conterá: a) o nome dos que nele apuseram assinatura digital; b) os identificadores das chaves públicas utilizadas para conferência das assinaturas e respectivas certificações que contiverem; c) a data das assinaturas; d) a declaração de que a cópia impressa confere com o original eletrônico e de que as assinaturas digitais foram conferidas pelo escrivão com o uso das chaves públicas acima indicadas; e) data e assinatura do escrivão.

Seção V – Da responsabilidade dos tabeliães

Art. 35 – O tabelião é responsável civilmente pelos danos diretos e indiretos sofridos pelos titulares dos certificados e quaisquer terceiros, em conseqüência do descumprimento, por si próprios, seus

prepostos ou substitutos que indicarem, das obrigações decorrentes do presente diploma e sua regulamentação. Seção VI – Dos Registros Eletrônicos

Art. 36 – O Registro de Título e Documentos fica autorizado a proceder à transcrição e ao registro de documentos eletrônicos particulares, para os fins previstos na Lei nº 6.015, de 31 de dezembro de 173. Parágrafo único – Poderá o Poder Judiciário autorizar o uso de documentos eletrônicos em atividades notariais e de registro não previstas expressamente na presente lei, adotando a regulamentação adequada, considerando inclusive as questões de segurança envolvidas.

Título V - Autoridades Competentes
Capítulo I – Do Poder Judiciário

Art. 37 - Compete ao Poder Judiciário: a) autorizar os tabeliães a exercerem atividade de certificação eletrônica; b) regulamentar o exercício das atividades de certificação, obedecidas as disposições desta lei; c) fiscalizar o cumprimento, pelos tabeliães, do disposto nesta lei e nas normas por ele adotadas, quanto ao exercício de suas funções; e d) impor as penalidades administrativas cabíveis, obedecido o processo legal, e independente das responsabilidades civis e penais dos tabeliães e seus oficiais. Parágrafo único: Não será deferida autorização ao exercício da atividade de certificação eletrônica a tabelião que não apresentar parecer técnico favorável emitido pelo Ministério da Ciência e Tecnologia.

Capítulo II – Do Ministério da Ciência e Tecnologia

Art. 38 – Compete ao Ministério de Ciência e Tecnologia: a) regulamentar os aspectos técnicos do exercício de atividade de certificação eletrônica pelos tabeliães, dispondo inclusive sobre os elementos que devam ser observados em seus planos de segurança; b) emitir parecer técnico sobre solicitação de tabelião para o exercício de atividade de certificação eletrônico; e c) emitir os certificados para chaves de assinatura que a serem utilizadas pelos tabeliães para firmarem certificados, devendo manter constantemente acessíveis ao público os certificados que tenha emitido, através de conexão por instrumentos de telecomunicações. Parágrafo primeiro – O Ministério da Ciência e Tecnologia revisará a cada 2 (dois) anos o regulamento técnico da certificação eletrônica, previsto na alínea a deste artigo, de forma a mantê-lo atualizado de acordo com os avanços da tecnologia. Parágrafo segundo - Não será emitido parecer técnico favorável ao solicitante que: a) não apresentar conhecimento ou as condições técnicas necessárias para o exercício de suas atividades; b) não apresentar plano de segurança, ou, apresentando-o, for ele indeferido, ou ainda, caso seja constatado que o plano por ele proposto não está adequadamente implantado em suas dependências e sistemas.

Art. 39 - Deverá o Ministério da Ciência e Tecnologia promover fiscalização em periodicidade adequada, quanto ao cumprimento, pelos tabeliães, das normas técnicas por ele adotadas. Parágrafo único - Apurando a fiscalização de que trata este artigo qualquer irregularidade no cumprimento das normas técnicas, deverá notificar o tabelião para apresentar defesa no prazo máximo de 5 (cinco) dias, bem como emitir, a propósito da defesa apresentada, manifestação fundamentada, em igual prazo, encaminhando os autos para o Poder Judiciário decidir.

Art. 40 – O tabelião deverá: a) documentar os sistemas que emprega na certificação, e as medidas constantes de seu plano de segurança, permitindo acesso a essa documentação pela fiscalização do Ministério de Ciência e Tecnologia; e b) documentar os certificados expedidos, vigentes, esgotados e revogados, permitindo acesso a essa documentação pela fiscalização do Poder Judiciário.

Título VI – Sanções Administrativas

Art. 41 - As infrações às normas estabelecidas nos Títulos IV e V desta lei, independente das sanções de natureza penal, e reparação de danos que causarem, sujeitam os tabeliães às seguintes penalidades: I - multa, de R$ 10.000,00 (dez mil reais) a R$ 1.000.000,00 (um milhão de reais); II - suspensão de certificado; III - cancelamento de certificado; IV - suspensão da autorização para exercício de atividade de certificação eletrônica; V - cassação da autorização para exercício de atividade de certificação eletrônica; V - cassação de licença de funcionamento.

Art. 42 - As sanções estabelecidas no artigo anterior serão aplicadas pelo Poder Judiciário, considerando-se a gravidade da infração, vantagem auferida, capacidade econômica, e eventual reincidência. Parágrafo único – As penas previstas nos incisos II e IV poderão ser impostas por medida cautelar antecedente ou incidente de procedimento administrativo.

Título VII - Sanções Penais

Art. 43 – Equipara-se ao crime de falsificação de papéis públicos, sujeitando-se às penas do art. 293 do Código Penal, a falsificação, com fabricação ou alteração, de certificado eletrônico público. Parágrafo primeiro - Incorre na mesma pena de crime de falsificação de papéis públicos quem utilizar certificado eletrônico público falsificado

Art. 44 – Equipara-se ao crime de falsificação de documento público, sujeitando-se às penas previstas no art. 297 do Código Penal, a falsificação, no todo ou em parte, de documento eletrônico público, ou alteração de documento eletrônico público verdadeiro. Parágrafo único – Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aplica-se o disposto no § 1º do art. 297 do Código Penal.

Art. 45 – Equipara-se ao crime de falsidade de documento particular, sujeitando-se às penas do art. 298 do Código Penal, a falsificação, no todo ou em parte, de documento eletrônico particular, ou alteração de documento eletrônico particular verdadeiro.

Art. 46 – Equipara-se ao crime de falsidade ideológica, sujeitando-se às penas do art. 299 do Código Penal, a omissão, em documento eletrônico público ou particular, de declaração que dele devia constar, ou a inserção ou fazer com que se efetue inserção, de declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Parágrafo único – Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aplica-se o disposto no parágrafo único do art. 299 do Código Penal.

Art. 47 – Equipara-se ao crime de falso reconhecimento de firma, sujeitando-se às penas do art. 300 do Código Penal, o reconhecimento, como verdadeira, no exercício de função pública, de assinatura eletrônica, que não o seja.

Art. 48 – Equipara-se ao crime de supressão de documento, sujeitando-se às penas do art. 305 do Código Penal, a destruição, supressão ou ocultação, em benefício próprio ou de outrem, de documento eletrônico público ou particular verdadeiro, de que não se poderia dispor.

Art. 49 – Equipara-se ao crime de extravio, sonegação ou inutilização de documento, sujeitando-se às penas previstas no art. 314 do Código Penal, o extravio de qualquer documento eletrônico, de que se tem a guarda em razão do cargo; ou sua sonegação ou inutilização, total ou parcial.

Título VIII - Disposições Gerais

Art. 50 - As certificações estrangeiras de assinaturas digitais terão o mesmo valor jurídico das expedidas no país, desde que entidade certificadora esteja sediada e seja devidamente reconhecida, em país signatário de acordos internacionais dos quais seja parte o Brasil, relativos ao reconhecimento jurídico daqueles certificados.

Parágrafo único - O Ministério da Ciência e Tecnologia fará publicar nos nomes das entidades certificadoras estrangeiras que atendam aos requisitos determinados neste artigo.

Art. 51 - Para a solução de litígios de matérias objeto desta lei poderá ser empregado sistema de arbitragem, obedecidos os parâmetros da Lei nº 9.037, de 23 de setembro de 1996, dispensada a obrigação decretada no § 2º de seu art. 4º, devendo, entretanto, efetivar-se destacadamente a contratação eletrônica da cláusula compromissória.

Título IX - Disposições Finais

Art. 52 - O Poder Executivo regulamentará a presente lei no prazo de 30 dias, após o qual deverão o Ministério da Ciência e Tecnologia e o Poder Judiciário, no prazo de 60 dias, baixar as normas necessárias para o exercício das atribuições conferidas pela presente lei. Art. 53 - A presente lei entrará em vigor no prazo de 180 dias da data de sua publicação.

PROJETO DE LEI DA CÂMARA N° 2.589 DE 15 DE MARÇO DE 2000

Autor: Dep. Edison Andrino

Altera o disposto no parágrafo único do art. 541 do Código de Processo Civil - Lei n° 5.869 de 11 de janeiro de 1973, para admitir as decisões disponíveis em mídia eletrônica, inclusive na Internet, entre as suscetíveis de prova de divergência jurisprudencial, para os fins do art. 105, III, alínea “c” da Constituição Federal.

O Congresso Nacional decreta:

Art. 1° - O parágrafo único do art. 541 do Código de Processo Civil, na redação que lhe deu a Lei n. 8.950, de 13.12.94, passa a vigorar com a seguinte redação:
“Parágrafo único - Quando o recurso fundar-se em dissídio jurisprudencial, o recorrente fará prova da divergência mediante certidão, cópia autenticada ou pela citação do repositório de jurisprudência, oficial ou credenciado, inclusive em mídia eletrônica, em que tiver sido publicada a decisão divergente, ou ainda pela reprodução de julgado disponível na Internet, com indicação da respectiva fonte, mencionando em qualquer caso as circunstâncias que identifiquem ou assemelhem os casos confrontados.”

Art. 2° - Esta lei entrará em vigor na data de sua publicação, revogadas as disposições em contrário.

EXCERTO DA CONSTITUIÇÃO FEDERAL REFERENTE AO CITADO PL

Art. 105. Compete ao Superior Tribunal de Justiça:

III - julgar, em recurso especial, as causas decididas, em única ou última instância, pelos Tribunais Regionais Federais ou pelos tribunais dos Estados, do Distrito Federal e Territórios, quando a decisão recorrida:

c) der a lei federal interpretação divergente da que lhe haja atribuído outro tribunal.

DECRETO Nº 3.585 DE 05 DE SETEMBRO DE 2000

Autor: Poder Executivo

Acresce dispositivo ao Decreto n. 2954, de 29 de janeiro de 1999, que estabelece regras para a redação de atos normativos de competência dos órgãos do Poder Executivo.

O PRESIDENTE DA REPÚBLICA , no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição,

DECRETA:

Art. 1º. O Decreto nº 2.954, de 29 de janeiro de 1999, passa a vigorar acrescido do seguinte artigo:

"Art. 57-A. A partir de 1º de janeiro de 2001, os documentos a que se refere este Decreto somente serão recebidos, na Casa Civil da Presidência da República, por meio eletrônico.

Art. 2º. Este Decreto entra em vigor na data de sua publicação.

DECRETO Nº 3.587 DE 05 DE SETEMBRO DE 2000

Autor: Poder Executivo

Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov. e dá outras providências.

O PRESIDENTE DA REPÚBLICA , no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição.

DECRETA:

CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Art. 1º. A Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov será instituída nos termos deste Decreto.

Art. 2º. A tecnologia da ICP-Gov deverá utilizar criptografia assimétrica para relacionar um certificado digital a um indivíduo ou a uma entidade.

§ 1º A criptografia utilizará duas chaves matematicamente relacionadas, onde uma delas é pública e, a outra, privada, para criação de assinatura digital, com a qual será possível a realização de transações eletrônica seguras e a troca de informações sensíveis e classificadas.

§ 2º A tecnologia de Chaves Públicas da ICP-Gov viabilizará, no âmbito dos órgãos e das entidades da Administração Pública Federal, a oferta de serviços de sigilo, a validade, a autenticidade e integridade de dados, a irrevogabilidade e irretratabilidade das transações eletrônicas e das aplicações de suporte que utilizem certificados digitais.

Art. 3º. A ICP-Gov deverá contemplar, dentre outros, o conjunto de regras e políticas a serem definidas pela Autoridade de Gerência de Políticas - AGP, que visem estabelecer padrões técnicos, operacionais e de segurança para os vários processos das Autoridades Certificadoras - AC, integrantes da ICP-Gov.

Art. 4º. Para garantir o cumprimento das regras da ICP-Gov, serão instituídos processos de auditoria, que verifiquem as relações entre os requisitos operacionais determinados pelas características dos certificados e os procedimentos operacionais adotados pelas autoridades dela integrantes.

Parágrafo único. Além dos padrões técnicos, operacionais e de segurança, a ICP-Gov definirá os tipos de certificados que podem ser gerados pelas AC.

CAPÍTULO II - DA ORGANIZAÇÃO DA ICP-GOV

Art. 5º. A arquitetura da ICP-Gov encontra-se definida no Anexo I a este Decreto.

Art. 6º. À Autoridade de Gerência de Políticas - AGP, integrante da ICP-Gov., compete:

I - propor a criação da Autoridade Certificadora Raiz - AC Raiz;
II - estabelecer e administrar as políticas a serem seguidas pelas AC;
III - aprovar acordo de certificação cruzada e mapeamento de políticas entre a ICP-Gov e outras ICP externas;
IV - estabelecer critérios para credenciamento das AC e das Autoridades de Registro - AR;
V - definir a periodicidade de auditoria nas AC e AR e as sanções pelo descumprimento de normas por ela estabelecidas;
VI - definir regras operacionais e normas relativas a:
a) Autoridade Certificadora - AC;
b) Autoridade de Registro - AR;
c) assinatura digital;
d) segurança criptográfica;
e) repositório de certificados;

f) revogação de certificados;
g) cópia de segurança e recuperação de chaves;
h) atualização automática de chaves;
i) histórico de chaves;
j) certificação cruzadas;
l) suporte a sistema para garantia de irretratabilidade de transações ou de operações eletrônica;
m) período de validade de certificado;
n) aplicações cliente;
VII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Gov. em especial da Política de Certificados - PC e das Práticas e Regras de Operação da Autoridade Certificadora, de modo a garantir:
a) atendimento às necessidades dos órgãos e das entidades da Administração Pública Federal;
b) conformidade com as políticas de segurança definidas pelo órgão executor da ICP-Gov; e
c) atualização tecnológica.

Art. 7º. Para assegurar a manutenção do grau de confiança estabelecido para a ICP-Gov, as AC e AR deverão credenciar-se junto a AGP, de acordo com as normas e os critérios por esta autoridade estabelecidos.

Art. 8º. Cabe à AC Raiz a emissão e manutenção dos certificados das AC de órgãos e entidades da Administração Pública Federal e das AC privadas credenciadas, bem como o gerenciamento da Lista de Certificados Revogados - LCR.

Parágrafo único. Poderão ser instituídos níveis diferenciados de credenciamento para as AC, de conformidade com a sua finalidade.

Art. 9º. As AC devem prestar os seguintes serviços básicos:

I - emissão de certificados;
II - revogação de certificados;
III - renovação de certificados;
IV - publicação de certificados em diretório;
V - emissão de Lista de Certificados Revogados - LCR;
VI - publicação de LCR em diretório; e
VII - gerência de chaves criptográficas.

Parágrafo único. A disponibilização de certificados emitidos e de LCR atualizada será proporcionada mediante uso de diretório seguro e de fácil acesso.

Art. 10. Cabe às AR:

I - receber as requisições de certificação ou revogação de certificado por usuário, confirmar a identidade destes usuários e a validade de sua requisição e encaminhar esses documentos à AC responsável;
II - entregar os certificados assinados pela AC aos seus respectivos solicitantes.

CAPÍTULO III - DO MODELO OPERACIONAL

Art. 11. A emissão de certificados será precedida de processo de identificação do usuário, segundo critérios e métodos variados, conforme o tipo ou em função do maior ou menor grau de sua complexidade.

Art. 12. No processo de credenciamento das AC, deverão ser utilizados, além de critérios estabelecidos pela AGP e de padrões técnicos internacionalmente reconhecidos, aspectos adicionais relacionados a:
I - plano de contingência;
II - política e plano de segurança, lógica e humana;
III - análise de riscos;
IV - capacidade financeira da proponente;
V - reputação e grau de confiabilidade da proponente e de seus gerentes;

VI - antecedentes e histórico no mercado; e
VII - níveis de proteção aos usuários dos seus certificados, em termos de cobertura jurídica e seguro contra danos.

Parágrafo único. O disposto nos incisos IV a VII não se aplica aos credenciamentos de AC Públicas.

Art. 13. Obedecidas às especificações da AGP, os órgãos e as entidades da Administração Pública Federal poderão implantar sua própria ICP ou ofertar serviços de ICP integrados à ICP-Gov.

Art. 14. A AC Privada, para prestar serviço à Administração Pública Federal, deve observar as mesmas diretrizes da AC Governamental, salvo outras exigências que vierem a ser fixadas pela AGP.

CAPÍTULO IV - DA POLÍTICA DE CERTIFICAÇÃO

Art. 15. Serão definidos tipos de certificados, no âmbito da ICP-Gov. que atendam às necessidades gerais da maioria das aplicações, de forma a viabilizar a interoperabilidade entre ambientes computacionais distintos, dentro da Administração Pública Federal.

§ 1º Serão criados certificados de assinatura digital e de sigilo, atribuindo-se-lhes os seguintes níveis de segurança, consoante o processo envolvido:

I - ultra-secretos;
II - secretos;
III - confidenciais;
IV - reservados; e
V - ostensivos.

§ 2º Os certificados, além de outros que a AGP poderá estabelecer, terão uso para:

I – assinatura digital de documentos eletrônicos;
II - assinatura de mensagem de correio eletrônico;
III - autenticação para acesso a sistemas eletrônicos; e
IV - troca de chaves para estabelecimento de sessão criptografada.

Art. 16. À AGP compete tomar as providências necessárias para que os documentos, dados e registros armazenados e transmitidos por meio eletrônico, óptico, magnético ou similar passem a ter a mesma validade, reconhecimento e autenticidade que se dá a seus equivalentes originais em papel.

CAPÍTULO V - DAS DISPOSIÇÕES FINAIS

Art. 17. Para instituição da ICP-Gov. deverá ser efetuado levantamento das demandas existentes nos órgãos governamentais quanto aos serviços típicos derivados da tecnologia de Chaves Públicas, tais como, autenticação, sigilo, integridade de dados e irretratabilidade das transações eletrônicas.

Art. 18. O Glossário constante do Anexo II apresenta o significado dos termos e siglas em português, que são utilizados no sistema de Chaves Públicas.

Art. 19. Compete ao Comitê Gestor de Segurança da Informação e concepção, a especificação e a coordenação da implementação da ICP-Gov, conforme disposto no art. 4º, inciso XIV, do Decreto nº 3.505, de 13 de junho de 2000.

Art. 20. Fica estabelecido o prazo de cento e vinte dias, contados a partir da data de publicação deste Decreto, para especificação, divulgação e início da implementação da ICP-Gov.

Art. 21. Implementados os procedimentos para a certificação digital de que trata este Decreto, a Casa Civil da Presidência da República estabelecerá cronograma com vistas à substituição progressiva do recebimento de documentos físicos por meios eletrônicos.

Art. 22. Este Decreto entra em vigor na data de sua publicação.

DECRETO Nº 3.714 DE 03 DE JANEIRO DE 2001

Autor: Poder Executivo

Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto nº 2.954, de 29 de janeiro de 1999, e dá outras providências.

O PRESIDENTE DA REPÚBLICA , no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição,

D E C R E T A :

Art. 1º. Para o cumprimento do disposto no art. 57-A do Decreto nº 2.954, de 29 de janeiro de 1999, serão observados os procedimentos estabelecidos neste Decreto.

Art. 2º. A transmissão dos documentos a que se refere este Decreto, assinados eletronicamente pela autoridade competente, far-se-á por sistema que lhes garanta a segurança, a autenticidade e a integridade de seu conteúdo, bem como a irretratabilidade ou irrecusabilidade de sua autoria.

Art. 3º. Cada Ministério criará caixa postal específica para recepção e remessa eletrônica de propostas dos atos a que se refere o Decreto nº 2.954, de 1999.

Parágrafo único. A Casa Civil da Presidência da República fixará o número de servidores que serão indicados e credenciados, pelos Ministros de Estado, para receber e dar destinação aos atos de que trata este artigo.

Art. 4º. A recepção dos documentos oficiais referidos no artigo anterior será objeto de confirmação mediante aviso de recebimento eletrônico.

Art. 5º. A caixa postal de que trata o art. 3º será dotada de dispositivo ou sistema de segurança que impeça a alteração ou a supressão dos documentos remetidos ou recebidos.

Art. 6º. O documento recebido na Casa Civil da Presidência da República será submetido ao Presidente da República para despacho, na forma estabelecida pelo Chefe da Casa Civil.

Art. 7º. Havendo necessidade de reprodução de documento em outro meio que não seja o eletrônico, o servidor responsável certificará a autenticidade da cópia ou reprodução.

Art. 8º. Cabe à Casa Civil da Presidência da República a administração do sistema a que se refere este Decreto aplicando-se, no que couber, o disposto no Decreto nº 3.587, de 5 de setembro de 2000.

Art. 9º. O Chefe da Casa Civil da Presidência da República poderá expedir normas complementares para cumprimento do disposto neste Decreto.

PROJETO DE LEI DO SENADO Nº 4.906-A DE 21 DE JUNHO DE 2001

Autor: Sen. Lúcio Alcântara com substitutivo do Dep. Júlio Semeguini

Dispõe sobre o comércio eletrônico.

O congresso Nacional decreta:

CAPÍTULO I
DO COMÉRCIO ELETRÔNICO EM GERAL
Seção Única
Disposições Preliminares

Art. 1º Esta lei, que regula o comércio eletrônico em todo o território nacional, aplica-se a qualquer tipo de informação na forma de mensagem eletrônica usada no contexto de atividades comerciais.

Art. 2º Considera-se, para os fins desta Lei:
I – mensagem eletrônica – a informação gerada enviada, recebida ou arquivada eletronicamente, por meio óptico ou por meios similares, incluindo, entre outros, "intercâmbio eletrônico de dados" (IED), correio eletrônico, telegrama, telex e fax;
II – intercâmbio eletrônico de dados (IED) – a transferência eletrônica, de computador para computador, de informações estruturadas de acordo com um padrão estabelecido para tal fim;
III – remetente de uma mensagem eletrônica – a pessoa pela qual, ou em cujo nome, a mensagem eletrônica é enviada ou gerada antes de seu armazenamento, caso este se efetue;
IV – destinatário de uma mensagem eletrônica – a pessoa designada pelo remetente para receber a mensagem eletrônica;
V – sistema de informação – é um sistema para geração, envio, recepção, armazenamento ou outra forma de processamento de mensagens eletrônicas.

Art. 3º Na interpretação desta Lei, levar-se-á em consideração a necessidade de promover a uniformidade da aplicação de normas sobre o comércio eletrônico em nível internacional.

Art. 4º Questões relativas a matérias regidas por esta Lei que nela não estejam expressamente disciplinadas serão solucionadas em conformidade, dentre outras, com os seguintes princípios gerais nos quais ela se inspira:
I – facilitar o comércio eletrônico interno e externo;
II – convalidar as operações efetuadas por meio de novas tecnologias da informação;
III – fomentar e estimular a aplicação de novas tecnologias da informação;
IV – promover a uniformidade do direito aplicável à matéria; e
V – apoiar as novas práticas comerciais.

CAPÍTULO II
DA APLICAÇÃO DE REQUISITOS LEGAIS ÀS MENSAGENS ELETRÔNICAS
Seção I
Do Reconhecimento Jurídico das Mensagens Eletrônicas

Art. 5º Serão reconhecidos os efeitos jurídicos, validade ou eficácia à informação sob a forma de mensagem eletrônica e àquela a que se faça remissão mediante a utilização dessa espécie de mensagem.

Seção II
Da Exigência de Informação Escrita e de Assinatura

Art. 6º Quando a lei determinar que uma informação conste por escrito, este requisito considerar-se-á por uma mensagem eletrônica, desde que a informação nela contida seja acessível para consulta posterior.

Art. 7º No caso de a lei exigir a assinatura de uma pessoa, este requisito considerar-se-á preenchido por uma mensagem eletrônica, desde que seja utilizado algum método para identificar a pessoa e indicar sua aprovação para a informação contida na mensagem.
Parágrafo único. O método utilizado deverá ser confiável e apropriado para os propósitos para os quais a mensagem for gerada ou comunicada, levando-se em consideração todas as circunstâncias do caso, inclusive qualquer acordo das partes a respeito.

Seção III
Da Exigência da Informação na forma Original

Art. 8º Quando a lei estabelecer que uma informação seja apresentado ou conservada na sua forma original, este requisito considerar-se-á preenchido por uma mensagem eletrônica, desde que:
I – haja garantia fidedigna de preservação de integridade da informação desde o momento de sua geração em sua forma final, como uma mensagem eletrônica ou de outra forma; e
II – a informação que seja acessível à pessoa a qual ela deva ser apresentada.
Parágrafo único. Para os propósitos do inciso II:
I – presume-se íntegra a informação que permaneça completa e inalterada, salvo a adição de qualquer endosso das partes ou outra mudança que ocorra no curso normal, da comunicação, armazenamento e exposição.
II – o grau de confiabilidade requerido será determinado à luz dos fins para os quais a informação for gerada, assim como de todas as circunstâncias do caso.

Seção IV
Da Exigência de Conservação das Mensagens Eletrônicas

Art. 9º Se a lei determinar que certos documentos, registro ou informações sejam conservados, este requisito considerar-se-á preenchido mediante a conservação de mensagens eletrônicas, desde que:
I - a informação que elas contenham seja acessível para consulta posterior;
II - as mensagens eletrônicas sejam conservadas no formato no qual tenham sido geradas, enviadas ou recebidas, ou num formato em que se possa demonstrar que representam exatamente as informações geradas, enviadas ou recebidas; e
III - se conserve, quando for o caso, toda informação que permita determinar a origem e o destino das mensagens e a data e hora em que foram enviadas ou recebidas.
Parágrafo único. A obrigação de conservar documentos, registros ou informações de acordo com o disposto neste artigo não se aplica àqueles dados que tenham por única finalidade facilitar o envio ou o recebimento da mensagem.

CAPÍTULO III
DA COMUNICAÇÃO DE MENSAGENS ELETRÔNICAS
Seção I
Da Alteração mediante Acordo

Art. 10 Nas relações entre as partes que geram, enviam, recebem, armazenam ou, de qualquer outro modo, processam mensagens eletrônicas, as disposições deste capítulo poderão ser alteradas mediante comum acordo.

Seção II
Da Celebração e Validade dos Contratos

Art. 11 Na celebração de um contrato, a oferta e sua aceitação podem ser expressas por mensagens eletrônicas.

Seção III
Do Reconhecimento das Mensagens Eletrônicas

Art. 12 Nas relações entre o remetente e o destinatário, se reconhecerá validade ou eficácia a uma declaração de vontade ou a qualquer outra declaração feita por meio de uma mensagem eletrônica.
Seção IV
Da Proveniência das Mensagens Eletrônicas

Art. 13 Nas relações entre o remetente e o destinatário, uma mensagem eletrônica será considerada proveniente do remetente quando ela for enviada.
I – pelo próprio remetente;
II – por uma pessoa autorizada a agir em nome do remetente;
III – por um sistema de informação programado pelo remetente, ou em seu nome para operar automaticamente.

§ 1º O destinatário tem ainda, direito a considerar uma mensagem eletrônica como proveniente do remetente:

I - quando aplicar corretamente um procedimento previamente aceito pelo remetente para verificar sua procedência; ou

II - quando a mensagem recebida resultar dos atos de uma pessoa cujas relações com o remetente ou com seus agentes lhe tenha dado acesso ao método usado pelo remetente para identificar as mensagens eletrônicas dele procedentes.

§ 2º O disposto no §1º não se aplicará:

I – a partir do momento em que o destinatário for informado pelo remetente de que a mensagem eletrônica não é de sua emissão; ou

II – nos casos previstos no inciso II do § 1º, desde o momento em que o destinatário saiba ou devesse saber, se agisse com a devida diligência, que a mensagem eletrônica não procede do remetente,

Art. 14. Presume-se que a mensagem eletrônica recebida corresponde àquela que o remetente pretendeu enviar, salvo quando o destinatário saiba ou devesse saber, se agisse com a devida diligência, ou empregasse o procedimento pactuado, que a transmissão causou algum erro na mensagem.

Art. 15. Presume-se que cada mensagem eletrônica recebida é uma mensagem distinta, salvo quando ela duplica uma outra e o destinatário saiba ou devesse saber, caso agisse com a devida diligência ou empregasse o procedimento pactuado, que se trata de duplicidade.

Seção V
Do Aviso de Recebimento

Art. 16. Os arts. 17, 18 e 19 aplicam-se quando, antes ou durante o envio de uma mensagem eletrônica, ou por meio desta mensagem, o remetente solicite ou pactue com o destinatário que este informe o seu recebimento.

Art. 17. Se o remetente não pactuar com o destinatário que este informe o recebimento de uma mensagem de uma forma ou por um método particular, poderá ser informado o seu recebimento mediante qualquer comunicação ou ato do destinatário que baste para esse propósito.

Art. 18. Quando o remetente declarar que os efeitos da mensagem eletrônica estão condicionados à recepção de um aviso de recebimento, a mensagem eletrônica considerar-se-á como não tendo sido enviada enquanto este não for recebido.

Art. 19. No caso de o remetente não declarar que os efeitos da mensagem eletrônica estão condicionados à recepção de um aviso de recebimento e tal aviso não for recebido pelo remetente dentro do prazo estabelecido ou pactuado, inexistindo este, o remetente poderá, em um prazo razoável:

I – notificar o destinatário declarando que nenhum aviso de recebimento foi recebido e estipulando um prazo adequando à efetivação desta providência;

II – caso o aviso de recebimento não seja recebido dentro do prazo a que se refere o inciso I, o remetente poderá, notificando o destinatário, tratar a mensagem como se ela nunca tivesse sido enviada.

Art. 20. A recepção, pelo remetente, do aviso de recebimento enviado pelo destinatário gera a presunção de que aquele tenha recebido a mensagem eletrônica pertinente.

Parágrafo único. A presunção a que se refere o caput não implica que a mensagem eletrônica corresponda à mensagem recebida.

Art. 21. Quando o aviso de recebimento o declarar, presume-se que a mensagem eletrônica cumpre os requisitos técnicos pactuados, ou previstos nas normas técnicas aplicáveis.

Seção VI
Do Tempo e Lugar de Despacho e Recebimento das Mensagens Eletrônicas

Art. 22. O envio de uma mensagem eletrônica ocorre quando esta entra em um sistema de informação alheio ao controle do remetente ou da pessoa que a envia em seu nome.

Art. 23. O momento de recepção de uma mensagem eletrônica é determinado:
I – quando o destinatário designar um sistema de informação para o propósito de recebimento das mensagens eletrônicas:
a) pelo momento em que a mensagem eletrônica entrar no sistema de informação designado; ou
b) pelo momento em que a mensagem eletrônica for recuperada pelo destinatário, no caso de ela ser enviada para um sistema de informação do destinatário que não seja o sistema de informação designado;
II – quando o destinatário não designar um sistema de informação, pelo momento em que a mensagem eletrônica entrar no sistema de informação do destinatário.
Parágrafo único. Aplica-se o disposto neste artigo ainda que o sistema de informação esteja situado num lugar distinto daquele em que a mensagem eletrônica se considere recebida de acordo com o disposto no art. 24.

Art. 24. Uma mensagem eletrônica se considera expedida e recebida nos locais onde o remetente e o destinatário têm seus estabelecimentos, respectivamente.
Parágrafo único. Para os fins do disposto neste artigo:
I – se o remetente ou o destinatário tem mais de um estabelecimento, considera-se aquele que guarda relação mais estreita com a transação subjacente ou, inexistindo esta, o seu estabelecimento principal;

II – se o remetente ou destinatário não possui estabelecimento, considera-se para os fins deste artigo, o local de sua residência habitual.

CAPÍTULO IV
DISPOSIÇÕES FINAIS

Art. 25. Esta Lei entra em vigor na data de sua publicação.

Art. 26. As disposições do Código Civil relativas à matéria objeto desta Lei, aplicam-se subsidiariamente, no que não contrariarem o que aqui se estatui.

MEDIDA PROVISÓRIA Nº 2.200, DE 28 DE JUNHO DE 2001

Autor: Poder Executivo

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º. Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º. A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º. A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por onze membros, sendo quatro representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e sete representantes dos seguintes órgãos, indicados por seus titulares:

I - Casa Civil da Presidência da República;

II - Gabinete de Segurança Institucional da Presidência da República;

III - Ministério da Justiça;

IV - Ministério da Fazenda;

V - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VI - Ministério do Planejamento, Orçamento e Gestão;

VII - Ministério da Ciência e Tecnologia.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º. O Comitê Gestor da ICP-Brasil será assessorado e receberá apoio técnico do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC.

Art. 5º. Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas para licenciamento das AC, das AR e dos demais prestadores de serviços de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, quando for o caso, certificar sua compatibilidade com a ICP-Brasil, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional;

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Art. 6º. À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, manter e cancelar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, cancelados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes estabelecidas pelo Comitê Gestor da ICP-Brasil.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 7º. O Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia é a AC Raiz da ICP-Brasil.

Parágrafo único. Para a consecução de seus objetivos, o Instituto Nacional de Tecnologia da Informação poderá, na forma da lei, contratar serviços de terceiros.

Art. 8º. Às AC, entidades autorizadas a emitir certificados digitais vinculando determinado código criptográfico ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados e as correspondentes chaves criptográficas, colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Art. 9º. Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 10. Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser licenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 11. É vedada a certificação de nível diverso do imediatamente subseqüente ao da autoridade certificadora, exceto nos casos de acordos de certificação lateral ou cruzada previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 12. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

Art. 13. A todos é assegurado o direito de se comunicar com os órgãos públicos por meio eletrônico.

Art. 14. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 15. Esta Medida Provisória entra em vigor na data de sua publicação.

DECRETO Nº 3.865 DE 13 DE JULHO DE 2001

(Revogado pelo DECRETO Nº 4.176, DE 28 DE MARÇO DE 2002)

Autor: Poder Executivo

Estabelece requisito para contratação de serviços de certificação digital pelos órgãos públicos federais, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição,

DECRETA:

Art. 1º. Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos da Administração Pública Federal, direta e indireta, e as entidades a eles vinculadas poderão contratar, para uso próprio ou de terceiros, quaisquer serviços de certificação digital de:

I - documentos em forma eletrônica;

II - aplicações de suporte; e

III - transações eletrônicas.

Parágrafo único. O Comitê Executivo do Governo Eletrônico poderá baixar normas complementares para cumprimento do disposto neste artigo e no art. 3º do Decreto de 18 de outubro de 2000, que o instituiu no âmbito do Conselho de Governo.

Art. 2º. Este Decreto entra em vigor na data de sua publicação.

DECRETO Nº 3.872 DE 18 DE JULHO DE 2001

Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição, e tendo em vista o disposto na Medida Provisória no 2.200, de 28 de junho de 2001,

DECRETA:

Art. 1o O Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, instituído pela Medida Provisória no 2.200, de 28 de junho de 2001, exerce a função de autoridade gestora de políticas (AGP) da referida Infra-Estrutura.

Art. 2o O CG ICP-Brasil, vinculado à Casa Civil da Presidência da República, é composto por onze membros, sendo quatro representantes da sociedade civil, integrantes de setores interessados e sete representantes dos seguintes órgãos, todos designados pelo Presidente da República:

I - Casa Civil da Presidência da República, que o coordenará;

II - Gabinete de Segurança Institucional da Presidência da República;

III - Ministério da Justiça;

IV - Ministério da Fazenda;

V - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VI - Ministério do Planejamento, Orçamento e Gestão; e

VII - Ministério da Ciência e Tecnologia.

§ 1o Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 2o A participação no CG ICP-Brasil é de relevante interesse público e não será remunerada.

§ 3o O CG ICP-Brasil terá uma Secretaria-Executiva.

§ 4o As decisões do CG ICP-Brasil serão aprovadas pela maioria absoluta de seus membros.

§ 5o Os membros do CG ICP-Brasil serão, em seus impedimentos, substituídos por suplentes designados na forma do caput.

§ 6o Poderão ser convidados a participar das reuniões do CG ICP-Brasil, a juízo do seu Coordenador ou do próprio Comitê, técnicos e especialistas de áreas afins.

Art. 3o Compete ao CG ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil;

II - estabelecer a política, os critérios e as normas para licenciamento das Autoridades Certificadoras - AC, das Autoridades de Registro - AR e dos demais prestadores de serviços de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da Autoridade Certificadora Raiz - AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, quando for o caso, certificar sua compatibilidade com a ICP-Brasil, negociar e aprovar, observados os tratados, acordos e atos internacionais, acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Art. 4º O CG ICP-Brasil será assistido e receberá suporte técnico da Comissão Técnica Executiva - COTEC, coordenada pelo Secretário-Executivo do Comitê Gestor, e integrada por representantes indicados pelos membros do CG ICP-Brasil e designados pelo Chefe da Casa Civil da Presidência da República.

§ 1º Serão convidados permanentes às reuniões da COTEC representantes:

I - do Ministério da Defesa;

II - do Ministério da Previdência e Assistência Social;

III - do Ministério da Saúde; e

IV - da Autoridade Certificadora Raiz - AC Raiz.

§ 2o Poderão ser convidados a participar das reuniões da COTEC, a juízo do seu Coordenador ou da própria Comissão, representantes de outros órgãos e entidades públicos.

§ 3º Compete à COTEC:

I - manifestar-se previamente sobre todas as matérias a serem apreciadas e decididas pelo CG ICP-Brasil;

II - preparar e encaminhar previamente aos membros do CG ICP-Brasil expediente contendo o posicionamento técnico dos órgãos e das entidades relacionados com as matérias que serão apreciadas e decididas; e

III - cumprir outras atribuições que lhe forem conferidas por delegação do CG ICP-Brasil.

§ 4º Os membros da COTEC serão, em seus impedimentos, substituídos por suplentes designados na forma do caput.

Art. 5º O CG ICP-Brasil estabelecerá a forma pela qual lhe será prestada assessoria pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC.

Art. 6º A Secretaria-Executiva do CG ICP-Brasil é chefiada por um Secretário-Executivo e integrada por assessores especiais e por pessoal técnico e administrativo.

§ 1º O Secretário-Executivo será designado por livre escolha do Presidente da República.

§ 2º A Secretaria-Executiva receberá da Casa Civil da Presidência da República o apoio necessário ao exercício de suas funções, inclusive no que se refere aos cargos de assessoria e ao apoio técnico e administrativo.

Art. 7º Compete à Secretaria-Executiva do CG ICP-Brasil:

I - prestar assistência direta e imediata ao Coordenador do Comitê Gestor;

II - preparar as reuniões do Comitê Gestor;

III - coordenar e acompanhar a implementação das deliberações e diretrizes fixadas pelo Comitê Gestor;

IV - coordenar os trabalhos da COTEC; e

V - cumprir outras atribuições que lhe forem conferidas por delegação do Comitê Gestor.

Art. 8o Este Decreto entra em vigor na data de sua publicação.

MEDIDA PROVISÓRIA Nº 2.200-1 DE 27 DE JULHO DE 2001

Autor: Poder Executivo

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º. Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º. A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º. A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º. O Comitê Gestor da ICP-Brasil será assessorado e receberá apoio técnico do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações CEPESC.

Art. 5º. Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil; II - estabelecer a política, os critérios e as normas técnicas para licenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados e regras operacionais, licenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Art. 6º. À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 7º. O Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia é a AC Raiz da ICP-Brasil.

Art. 8º. Às AC, entidades autorizadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 9º. Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 10. Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser licenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 11. É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 12. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não

emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 13. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 14. Para a consecução dos seus objetivos, o Instituto Nacional de Tecnologia da Informação poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Ministro de Estado da Ciência e Tecnologia poderá requisitar, para ter exercício exclusivo no Instituto Nacional de Tecnologia da Informação, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou entidade de origem.

§ 3º Fica o Ministério da Ciência e Tecnologia autorizado a custear as despesas com remoção e estada para os servidores que, em virtude de nomeação para cargos em comissão no Instituto Nacional de Tecnologia da Informação, vierem a ter exercício em cidade diferente da de seu domicílio, observados os limites de valores estabelecidos para a Administração Pública Federal direta.

Art. 15. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200, de 28 de junho de 2001.

Art. 16. Esta Medida Provisória entra em vigor na data de sua publicação.

MEDIDA PROVISÓRIA Nº 2.200-2 DE 24 DE AGOSTO DE 2001

Autor: Poder Executivo

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O PRESIDENTE DA REPÚBLICA , no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º. Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º. A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º. A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º. Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;
II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º. À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º. Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º. Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º. Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º. É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11. A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12. Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13. O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14. No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15. Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.

Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16. Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17. Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação do Ministério da Ciência e Tecnologia;

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei nº 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18. Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19. Ficam convalidados os atos praticados com base na Medida Provisória nº 2.200-1, de 27 de julho de 2001.

Art. 20. Esta Medida Provisória entra em vigor na data de sua publicação.

DECRETO Nº 3.996 DE 31 DE OUTUBRO DE 2001

Autor: Poder Executivo

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

O VICE-PRESIDENTE DA REPÚBLICA, no exercício do cargo de Presidente da República, usando das atribuições que lhe confere o art. 84, incisos II, IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

DECRETA:

Art. 1º. A prestação de serviços de certificação digital no âmbito da Administração Pública Federal, direta e indireta, fica regulada por este Decreto.

Art. 2º. Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, os órgãos e as entidades da Administração Pública Federal poderão prestar ou contratar serviços de certificação digital.

§ 1º Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil.

§ 2º Respeitado o disposto no § 1º, o Comitê Executivo do Governo Eletrônico poderá estabelecer padrões e requisitos administrativos para a instalação de Autoridades Certificadoras - AC e de Autoridades de Registro AR próprias na esfera da Administração Pública Federal.

§ 3º As AR de que trata o § 2º serão, preferencialmente, os órgãos integrantes do Sistema de Administração do Pessoal Civil - SIPEC.

Art. 3º. A tramitação de documentos eletrônicos para os quais seja necessária ou exigida a utilização de certificados digitais somente se fará mediante certificação disponibilizada por AC integrante da ICP-Brasil.

Art. 4º. Será atribuída, na Administração Pública Federal, aos diferentes tipos de certificados disponibilizados pela ICP-Brasil, a classificação de informações segundo o estabelecido na legislação específica.

Art. 5º. Este Decreto entra em vigor na data de sua publicação.

Art. 6º. Fica revogado o Decreto nº 3.587, de 5 de setembro de 2000.

RETIFICAÇÃO - DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001

(Publicado no Diário Oficial da União de 5 de novembro de 2001, Seção 1, página 2)
No art. 2:
onde se lê: "Somente mediante prévia autorização do Comitê Gestor do Governo Eletrônico, ..."
leia-se: "Somente mediante prévia autorização do Comitê Executivo do Governo Eletrônico, .."

DECRETO Nº 4.176 DE 28 DE MARÇO DE 2002

Autor: Poder Executivo

Revoga os decretos 2.954 e 3.585

Estabelece normas e diretrizes para a elaboração, a redação, a alteração, a consolidação e o encaminhamento ao Presidente da República de projetos de atos normativos de competência dos órgãos do Poder Executivo Federal, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto na Lei Complementar nº 95, de 26 de fevereiro de 1998,

DECRETA:

Objeto e Âmbito de Aplicação

Art. 1º Este Decreto estabelece normas e diretrizes para a elaboração, a redação, a alteração e a consolidação de atos normativos a serem encaminhados ao Presidente da República pelos Ministérios e órgãos da estrutura da Presidência da República.

Parágrafo único. Consideram-se atos normativos para efeitos deste Decreto as leis, as medidas provisórias e os decretos.

...

Capítulo II

DO ENCAMINHAMENTO E DO EXAME DOS PROJETOS DE ATO NORMATIVO

Encaminhamento de Projetos

Art. 37. As propostas de projetos de ato normativo serão encaminhadas à Casa Civil por meio eletrônico, com observância do disposto no Anexo I, mediante exposição de motivos do titular do órgão proponente, à qual se anexarão:

OBS: O texto deste decreto é de volume razoável e para tanto foram expostos somente os artigos relevantes ao tema do presente trabalho para fins de clareza e concisão.

PROJETO DE LEI DA CÂMARA N° 6.965 DE 12 DE JUNHO DE 2002

Autor: Dep. José Carlos Coutinho

“Confere valor jurídico à digitalização de documentos, e dá outras providências.”

O Congresso Nacional decreta:

Art.1º Fica autorizado, em todo o território nacional, o armazenamento de informações, dados e imagens que constituem o acervo documental das empresas privadas e órgãos públicos federais, estaduais, municipais e do Distrito Federal, em sistemas eletrônicos digitais que, uma vez gravados, garantam o nível de segurança exigido.

Parágrafo único - A utilização do sistema dependerá de disciplinamento no respectivo regimento interno da instituição pública ou sistemática de arquivamento da empresa privada, desde que ambos atendam ao decreto regulamentador específico.

Art.2º As unidades da administração pública e as empresas privadas que se utilizam do arquivamento digitalizado procederão ao controle desses mesmo documentos à conversão.

§1º O controle dos documentos digitalizados será feito em livro, sistema de fichas, sistema eletrônico, ou outros, da conveniência da unidade administrativa ou da empresa, desde que permita sua rápida localização.

§2º Os documentos digitalizados utilizarão obrigatoriamente um sistema de indexação que permita sua rápida recuperação.

Art.3º Terão valor jurídico as cópias em papel obtidas do sistema de armazenamento digitalizado, quando chancelados pelo órgão competente da repartição pública ou empresa privada que as produziram.

Art.4º Ressalvados os termos codificados como segredo de justiça, é garantido a qualquer cidadão o direito de acesso às informações digitais armazenadas em órgãos públicos, delas podendo ser extraídas certidões ou reproduzidos os documentos, a requerimento do interessado.

Art.5º Os originais dos documentos convertidos ao sistema digitalizado serão destruídos por meio de comprovada eficácia respeitando-se os prazos previstos para a prescrição dos documentos mencionados nas tabelas oficiais de temporalidade definidas pelo Governo e pelo Conarc.

Parágrafo único - É permitida a destruição dos documentos antes do prazo prescricional se o mesmo estiver contido em mídia de valor legal como o microfilme.

Art.6º O Art. 365 da Lei nº 5.869, de 11 de janeiro de 1973, fica acrescido do seguinte inciso:

“Art. 365 ....

IV- Os documentos públicos reproduzidos a partir de arquivo digitalizado, desde que chancelados pelo órgão competente e pelo servidor designado para esse fim.”

Art.7º Esta lei entra em vigor na data de sua publicação.

Art.8º Revogam-se as disposição em contrário.

PROJETO DE LEI DA CÂMARA N.º 7.093 DE 6 DE AGOSTO DE 2002

Autor: Dep. Ivan Paixão

Esta lei dispõe sobre a correspondência eletrônica comercial, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta lei dispõe sobre a correspondência eletrônica comercial, proporciona aos receptores a escolha de parar de receber mensagens eletrônicas comerciais e estabelece sanções administrativas e penais aplicáveis.

Art. 2º Para os efeitos desta lei, considera-se:
I – mensagem eletrônica comercial: qualquer mensagem eletrônica enviada a um receptor cujo propósito seja divulgar ou promover, por propósito comercial, produto ou serviço, incluindo conteúdo de site da internet ou, ainda, à propagação de correntes ou pirâmides;
II – remetente: pessoa que inicia uma mensagem eletrônica comercial;
III - receptor: destinatário de uma mensagem eletrônica comercial;
IV - correntes ou pirâmides: correspondência eletrônica destinada a obtenção de recursos financeiros mediante incentivo para que o receptor reenvie a mensagem a outros usuários da internet.
V –computador protegido: aquele que é usado pelo cidadão comum, por instituição financeira, pelo governo, ou aquele que é utilizado para fins comerciais;
VI – endereço eletrônico: destinação, usualmente expressa por uma seqüência de caracteres, para qual correspondência eletrônica pode ser enviada;
VII – informação do cabeçalho: fonte, destinação e sinalização da rota da informação anexada ao início de mensagem eletrônica, incluindo o nome de domínio e endereço eletrônico originários.
VIII – nome de domínio: qualquer designação alfanumérica registrada ou atribuída por qualquer registrador, estabelecimento de nome de domínio ou outra autoridade de inscrição de nome de domínio como parte de um endereço eletrônico na internet;
IX – transmissão rotineira: transmissão, envio, transmissão em cadeia, manuseio ou armazenagem, através de processo técnico automático, de mensagem eletrônica;
§1º A mensagem eletrônica não deve ser considerada puramente comercial por incluir referência a uma entidade comercial que serve para identificar o remetente ou uma referência ou link de site da internet operado com propósito comercial.
§ 2º Não se enquadra na definição de remetente a pessoa, inclusive um provedor de acesso a internet, cujo o papel com respeito a mensagem seja limitado a transmissão rotineira da mensagem.
§ 3º Se o destinatário da mensagem eletrônica comercial tiver um ou mais endereços eletrônicos, além daquele ao qual a mensagem for dirigida, será tratado como receptor separado com respeito a cada um desses endereços.

Art. 3º Há direito de liberdade de expressão na Internet.

Art. 4º A mensagem eletrônica comercial não pode conter informação falsa, enganosa ou não obtida legitimamente.

Art. 5º Para iniciar a transmissão de uma mensagem eletrônica comercial a um computador protegido, tal mensagem deve conter, de maneira clara e evidente, para o receptor:
I – a identificação de que a mensagem é uma propaganda ou solicitação;
II – o nome, endereço físico, endereço eletrônico e número de telefone do remetente;
III – aviso ao receptor sobre a oportunidade de recusa a receber mais mensagens eletrônicas comerciais do remetente.
§ 1º O remetente de uma mensagem eletrônica comercial não solicitada deve manter um endereço eletrônico em funcionamento, através do qual o receptor possa manifestar a recusa de não mais receber mensagens.
§ 2º O remetente, ou qualquer pessoa agindo em seu nome, tem o prazo de 24 horas do recebimento da recusa do receptor para encerrar a transmissão de correspondência eletrônica comercial.

Art. 6º Os provedores de serviços de Internet podem estabelecer uma política sobre a entrada de correspondência eletrônica comercial não solicitada em seus servidores.

Art. 7º A comercialização de listas de endereços eletrônicos, compilações de informações e afins somente é permitida após autorização prévia dos usuários da internet.

Art. 8º O Poder Público designará uma autoridade, a quem caberá:
I - a fiscalização e repressão ao envio indevido de mensagem eletrônica comercial e a comercialização de listas de endereços eletrônicos, compilações de informações e afins;
II – disponibilização de um banco de dados para cadastrar os endereços eletrônicos de usuários que não desejam receber nenhum tipo de correspondência eletrônica comercial.
Parágrafo único Para enviar qualquer mensagem aos endereços constantes do banco de dados do Poder Público, o remetente deverá ter recebido autorização prévia do receptor.

Art. 9º As infrações aos preceitos desta lei constituem crime e sujeitam os responsáveis à pena de reclusão, de um a quatro anos.

Art. 10 As infrações aos preceitos desta lei, independente das sanções de natureza penal e reparação de danos que causarem, sujeitam o infrator à pena de multa de cem a dez mil reais por mensagem enviada, acrescida de um terço na reincidência.

Art. 11 Aplicam-se as normas de defesa e proteção do consumidor vigente no País, naquilo que não conflitar com esta lei.

Art. 12 Esta lei entra em vigor em cento e vinte dias, contados da data de sua publicação.

DECRETO Nº 4.414 DE 07 DE OUTUBRO DE 2002

Autor: Poder Executivo

Altera o Decreto nº 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos II e VI, alínea "a", da Constituição,

D E C R E T A :

Art. 1º. O Decreto nº 3.996, de 31 de outubro de 2001 passa a vigorar acrescido do seguinte artigo:

"Art. 3º-A . As aplicações e demais programas utilizados no âmbito da Administração Pública Federal direta e indireta que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer AC integrante da ICP-Brasil. " (NR)

Art. 2º. Este Decreto entra em vigor na data de sua publicação.

PROJETO DE LEI DO EXECUTIVO Nº 7.316 DE 7 DE NOVEMBRO DE 2002
Autor: Poder Executivo

Disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação.

O Congresso Nacional decreta:

Art. 1º O uso de assinaturas eletrônicas e a prestação de serviços de certificação rege-se por esta Lei.

Art. 2º Para os fins desta Lei, entende-se por:
I – assinatura eletrônica, o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como meio de comprovação de autoria;
II – assinatura eletrônica avançada, a assinatura eletrônica que:
a) esteja associada inequivocamente ao seu titular, permitindo a sua identificação;
b) seja produzida por dispositivo seguro de criação de assinatura;
c) esteja baseada em certificado qualificado válido à época de sua aposição; e
d) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer lteração subseqüente no conteúdo desse seja plenamente detectável;
III – chave de criação de assinatura, o conjunto único de dados eletrônicos, tal como chaves criptográficas privadas, utilizado pelo seu titular para a criação de uma assinatura eletrônica;
IV – chave de verificação de assinatura, o conjunto de dados eletrônicos, tal como chaves criptográficas públicas, utilizado para verificar uma assinatura eletrônica;
V – dispositivo seguro de criação de assinaturas, o dispositivo físico (hardware) e lógico (software) destinado a viabilizar o uso da chave de criação de assinatura que, na forma do regulamento:
a) assegure a confidencialidade dessa;
b) inviabilize a dedução dessa a partir de outros dados;
c) permita ao legítimo titular dessa protegê-la de modo eficaz contra o seu uso por terceiros;
d) proteja a assinatura eletrônica contra falsificações; e
e) não modifique o documento eletrônico a ser assinado, nem impeça a sua apresentação ao titular antes do processo de assinatura;

VI – certificado, o atestado eletrônico que vincula uma chave de verificação de assinatura a uma pessoa, identificando-a;
VII – certificado qualificado, o certificado emitido por prestador de serviços de certificação credenciado que contenha, ao menos:
a) o seu número de série;
b) o nome do seu titular e a sua respectiva chave de verificação de assinatura;
c) a identificação e a assinatura eletrônica avançada do prestador de serviços de certificação que o emitiu;
d) a data de início e de fim do prazo de validade do certificado;
e) as restrições ao âmbito de utilização do certificado, se for o caso; e
f) outros elementos definidos em regulamento e nas normas complementares a esta Lei;

VIII – prestador de serviços de certificação, a pessoa jurídica que emite certificados ou presta outros serviços relacionados com assinaturas eletrônicas;

IX – prestador de serviços de certificação credenciado, o prestador de serviço de certificação titular de certificado emitido na forma do art. 5o, § 1o;

X – componentes de aplicação de assinatura, os produtos físicos (hardware) e lógicos (software) que:
a) vinculem ao documento eletrônico processo de produção ou verificação de assinaturas eletrônicas; ou
b) verifiquem assinaturas eletrônicas ou confiram certificados, disponibilizando os resultados; e

XI – componentes técnicos para serviços de certificação, os produtos físicos (hardware) e lógicos (software) que:
a) gerem chaves de assinatura, transferindo-as para um dispositivo seguro de criação de assinatura; ou
b) mantenham certificados disponíveis ao público para verificação e, caso necessário, obtenção por rede de computadores.
Parágrafo único. É condição para emissão de certificados qualificados, a identificação e o cadastramento de seu titular mediante a sua presença física.

Art. 3º Observado o disposto nesta Lei, a prestação de serviços de certificação não se sujeita à prévia autorização pelo Poder Público.

Art. 4º As assinaturas eletrônicas avançadas têm o mesmo valor jurídico e probante da assinatura manuscrita.
§ 1º As declarações constantes dos documentos em forma eletrônica que contenham assinatura eletrônica avançada presumem-se verdadeiras em relação ao seu titular.
§ 2º Os atos que exijam forma especial, bem como aqueles sujeitos aos serviços de que trata a Lei no 8.935, de 18 de novembro de 1994, quando formalizados em meio eletrônico, deverão ser, sob pena de nulidade, assinados mediante a aposição de assinatura eletrônica avançada.
§ 3º Não serão negados efeitos jurídicos à assinatura eletrônica, nem será excluída como meio de prova, em virtude de se apresentar em forma eletrônica, de não estar baseada num certificado qualificado ou de não ter sido gerada através de dispositivo seguro de criação de assinaturas, desde que admitida pelas partes como válida ou aceita pela pessoa a quem foi oposta.

Art. 5º Mediante requerimento a ser encaminhado à Autoridade Certificadora Raiz – AC Raiz da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, o prestador de serviços de certificação poderá ser credenciado, desde que, na forma do regulamento:
I – comprove o cumprimento das diretrizes e normas técnicas, bem como das regras operacionais e práticas de certificação editadas pelo Comitê Gestor e pela AC Raiz da ICP-Brasil na forma da Medida Provisória no 2.200-2, de 24 de agosto de 2001;
II – mantenha contrato de seguro em vigor para cobertura total da responsabilidade civil decorrente da atividade de certificação;
III – disponha de profissionais que comprovadamente tenham o conhecimento, a experiência e a qualificação necessários ao exercício da atividade;
IV – garanta a confidencialidade da chave de criação de assinatura de modo que o seu uso, conhecimento e controle sejam exclusivos do seu titular;
V – demonstre possuir mecanismos e procedimentos adequados a impedir a falsificação ou deturpação de certificados;
VI – utilize sistema seguro de armazenamento de certificados de modo que:
a) apenas as pessoas autorizadas possam introduzir-lhe dados e alterações;
b) a autenticidade das informações possa ser verificada; e
c) os certificados possam ser conferidos pelo público apenas quando consentido pelo seu titular;

VII – possua sistemas de proteção de dados adequados para impedir o uso indevido de informações e documentos fornecidos pelo titular para emissão do certificado;

VIII – suas instalações operacionais e seus recursos de segurança física e lógica sejam compatíveis com a atividade de certificação e estejam localizados no território nacional;
IX – assegure que seus órgãos de registro realizam a identificação e o cadastramento dos usuários somente mediante a presença física desses, bem como mantenham os documentos por eles fornecidos pelo período de tempo necessário;
X – implemente práticas eficazes de informação do usuário, inclusive sobre os efeitos jurídicos produzidos pelo certificado emitido e as medidas necessárias para proteção e segurança da chave de criação de assinatura;
XI – garanta o funcionamento de diretório rápido e seguro e de serviço de revogação de certificados seguro e imediato;
XII – assegure com precisão a possibilidade de verificação da data e hora de emissão ou revogação de cada certificado;
XIII – utilize componentes de aplicação de assinatura e componentes técnicos para serviços de certificação que atendam os requisitos definidos nos arts. 12 e 13 desta Lei, e tenham sido previamente testados e aprovados; e
XIV – utilize sistemas e produtos seguros que estejam protegidos contra modificações e garantam a segurança técnica e criptográfica dos processos para os quais estejam previstos;
§ 1º O credenciamento importa necessariamente na emissão do certificado do prestador de serviços de certificação pela AC Raiz da ICP-Brasil ou por prestadora de serviços de certificação credenciada na forma deste artigo.
§ 2º O credenciamento poderá ser limitado no tempo e a determinados tipos de certificados.
§ 3º Somente os certificados contemplados pelo ato de credenciamento poderão constituir certificados qualificados, observado o disposto no art. 2o, VII, desta Lei.
§ 4º A inobservância de qualquer dos requisitos previstos neste artigo implicará o cancelamento do ato de credenciamento e a imediata revogação do respectivo certificado, sem prejuízo das demais sanções cabíveis.

Art. 6º O disposto no art. 5o aplica-se, no que couber, ao credenciamento de provedores de serviços de certificação de data e hora, bem como de outros serviços e aplicações de suporte.

Art. 7º O credenciamento de um prestador de serviços de certificação importa na atribuição do selo de qualidade da ICP-Brasil.
§ 1º É de uso exclusivo dos prestadores de serviços de certificação certificados na forma do § 1o do art. 5o a designação “Prestador de Serviços de Certificação Credenciado”.
§ 2º O certificado emitido por prestador de serviços de certificação credenciado na forma do art. 5o conterá a informação de que é um “certificado qualificado”, sendo vedado o emprego dessa expressão para designar quaisquer outros certificados.
§ 3º Os certificados qualificados emitidos na forma desta Lei constituem documentos oficiais de identificação em meio eletrônico.
§ 4º As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer prestador de serviço de certificação credenciado na forma do art. 5o.

Art. 8º Os prestadores de serviços de certificação informarão seus usuários das medidas necessárias para a manutenção da segurança de assinaturas eletrônicas e sua verificação de modo confiável.
§ 1º Será fornecido, na forma do caput, documento informativo ao usuário que confirmará que o leu e tomou ciência de seu conteúdo, por meio de termo formalizado em papel devidamente assinado.
§ 2º Os prestadores de serviços de certificação informarão aos usuários que uma assinatura eletrônica avançada, nos termos desta Lei, produz os efeitos descritos no art. 4o.

§ 3º O par de chaves de assinatura será gerado sempre pelo próprio titular, e sua chave de criação de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 9º Deve o prestador de serviços de certificação revogar um certificado:
I – mediante solicitação do seu titular ou representante constituído;
II – caso o certificado tenha sido emitido com base em dados falsos;
III – caso o prestador de serviços de certificação tenha encerrado suas atividades sem que fossem prosseguidas por um outro prestador de serviços de certificação;
IV – por determinação da AC Raiz da ICP-Brasil, caso o prestador de serviços de certificação seja credenciado na forma do art. 5o; ou
V – em outros casos definidos em regulamento e nas normas complementares a esta Lei.

Art. 10. O prestador de serviço de certificação responde:
I – diretamente, pelos danos a que der causa; e
II – solidariamente, pelos danos que derem causa os prestadores de serviços de certificação por ele diretamente certificados, bem como os órgãos de registro e os prestadores de serviços de suporte a ele vinculados.

Parágrafo único. Se constar do certificado qualificado restrições ao uso da assinatura eletrônica avançada, na forma do art. 2o, VII, "e", os danos causados são indenizáveis dentro dos limites dessas restrições.

Art. 11. A intenção do prestador de serviços de certificação de encerrar suas atividades será comunicada, com, no mínimo, dois meses de antecedência, indicando o prestador que o sucederá ou o momento em que serão revogados os certificados:
I – às pessoas a quem tenha emitido certificados que estejam em vigor; e
II – à AC Raiz da ICP-Brasil, caso seja credenciado.
§ 1o A comunicação prevista no caput será imediata, nas hipóteses de falência ou liquidação extrajudicial.
§ 2º O prestador de serviços de certificação transferirá, se for o caso, a documentação relativa aos certificados digitais emitidos ao prestador que os tenha assumido.
§ 3º Caso os certificados qualificados não tenham sido assumidos por outro prestador de serviços de certificação credenciado, os documentos de que trata o parágrafo anterior serão repassados à AC Raiz da ICP-Brasil.

Art. 12. A assinatura de documentos eletrônicos, decorrente de certificados qualificados, exige componentes de aplicação de assinatura que claramente indiquem a produção de uma assinatura eletrônica, e permita a identificação do documento a que a assinatura se refere.

Parágrafo único. Para conferir o documento assinado, os componentes de aplicação de assinatura, na forma do regulamento, devem demonstrar:
I – a que documento a assinatura se refere;
II – se o documento não foi modificado;
III – a que titular de certificado está vinculado o documento; e
IV – o conteúdo do certificado em que está baseada a assinatura.

Art. 13. Os componentes técnicos para serviços de certificação conterão, na forma do regulamento, mecanismos que:
I – assegurem que as chaves de criação de assinatura produzidas e transferidas a dispositivo seguro de criação de assinatura sejam únicas e sigilosas; e

II – protejam os certificados que estejam disponíveis para verificação e obtenção na rede de alterações, cópias ou obtenções (download) não autorizadas.

Art. 14. Fica assegurado ao certificado emitido no exterior os mesmos efeitos do certificado de que trata o inciso VI do art. 2o.

Parágrafo único. Tratados, acordos ou atos internacionais poderão atribuir aos certificados emitidos no exterior os mesmos efeitos do certificado de que trata o inciso VII do art. 2o, observado o princípio da reciprocidade.

Art. 15. A infração de qualquer dispositivo desta Lei sujeita o responsável, sem prejuízo de outras sanções, à multa variável de cinqüenta mil reais a um milhão de reais, segundo o regulamento.
§ 1º Cabe à AC Raiz da ICP-Brasil executar a fiscalização e auditoria dos prestadores de serviços de certificação credenciados, autuá-los, aplicar as penalidades de advertência, por escrito, e ainda as multas e medidas administrativas cabíveis, notificando os infratores e arrecadando as multas que aplicar.
§ 2º Regulamento disporá sobre:
I – as medidas administrativas cabíveis, especialmente sobre revogação compulsória de certificados, cessação e suspensão dos serviços de certificação; e
II – o poder de supervisão da AC Raiz da ICP-Brasil em relação aos demais prestadores de serviços de certificação, a ser exercido na forma deste artigo.
§ 3º Aplica-se, no que couber, à prestação de serviços de certificação a legislação de defesa do consumidor.

Art. 16. O Poder Executivo disporá, ainda, sobre o uso de certificados digitais na emissão de passaportes, de documentos de identidade, de carteiras de habilitação de condutores de veículos, de certificados de registros de veículos e em outras aplicações, bem como sobre a emissão de certificados de atributos.

Art. 17. As referências normativas a Autoridades Certificadoras – AC passam a ser entendidas como prestadores de serviços de certificação credenciados, exceto no caso da AC Raiz da ICP-Brasil.
Art. 18. O disposto no § 2o do art. 4o não dispensa a manutenção, em papel ou microfilme, dos livros de registros públicos ou das fichas que os substituam, na forma da legislação vigente, em especial do art. 22 da Lei no 6.015, de 31 de dezembro de 1973.

Art. 19. Ficam mantidas as competências do Comitê Gestor da ICP-Brasil e da AC Raiz da ICP-Brasil, na forma da Medida Provisória no 2.200-2, de 24 de agosto de 2001, salvo disposição regulamentar em contrário.

Parágrafo único. Os certificados emitidos até a edição desta Lei permanecem válidos, na forma da Medida Provisória no 2.200-2, de 24 de agosto de 2001.

Art. 20. Esta Lei entra em vigor na data de sua publicação.

SUBSTITUTIVO AO PROJETO DE LEI Nº 7.316 DE 7 DE NOVEMBRO DE 2002

(Consolidado e atualizado com todas as emendas aprovadas deste projeto, nos termos do Substitutivo da CCTCI, com subemendas; e das Emendas apresentadas nesta Comissão de nºs 1, com subemenda; 2, com subemenda; e 3 a 12)

Autor: Poder Executivo

Dispõe sobre o uso de assinaturas eletrônicas e certificados digitais, a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, a prestação de serviços de certificação e dá outras providências.

O CONGRESSO NACIONAL decreta:

TÍTULO I - DAS ASSINATURAS ELETRÔNICAS E DOS CERTIFICADOS DIGITAIS

CAPÍTULO I - DAS DISPOSIÇÕES GERAIS

Art. 1º Esta lei estabelece normas sobre o uso de assinaturas eletrônicas e certificados digitais, a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, a prestação de serviços de certificação e dá outras providências.

Art. 2º Para os fins desta Lei, entende-se por:
I – documento eletrônico, uma seqüência de bits elaborada mediante processamento eletrônico de dados, destinada a reproduzir uma manifestação do pensamento ou um fato;
II - assinatura eletrônica, o conjunto de dados sob forma eletrônica, ligados ou logicamente associados a outros dados eletrônicos, utilizado como método de comprovação da autoria;
III – assinatura eletrônica avançada, a assinatura eletrônica que:
a) esteja associada inequivocamente a um par de chaves criptográficas que permita identificar o signatário;
b) seja produzida por dispositivo seguro de criação de assinatura;
c) esteja vinculada ao documento eletrônico a que diz respeito, de tal modo que qualquer alteração subseqüente neste seja plenamente detectável; e
d) esteja baseada em um certificado qualificado e válido à época da sua aposição;
IV – chave de criação de assinatura, o conjunto único de dados eletrônicos, tal como chaves criptográficas privadas, utilizado para a criação de uma assinatura eletrônica;
V – chave de verificação de assinatura, o conjunto de dados eletrônicos, tal como chaves criptográficas públicas, utilizado para a verificação de uma assinatura eletrônica;
VI – dispositivo seguro de criação de assinaturas, o dispositivo físico (hardware) e lógico (software) destinado a viabilizar o uso da chave de criação de assinatura que, na forma do regulamento:
a) assegure a confidencialidade desta;
b) inviabilize a dedução desta a partir de outros dados;
c) permita ao titular ou responsável pelo uso do certificado proteger a chave de criação de assinatura, de modo eficaz contra o seu uso por terceiros;
d) proteja a assinatura eletrônica contra falsificações; e
e) não modifique o documento eletrônico a ser assinado;
VII – certificado, o documento eletrônico que vincula uma chave de verificação de assinatura a uma pessoa, identificando-a;
VIII – certificado qualificado, o certificado emitido por prestador de serviços de certificação credenciado pela ICP-Brasil, que contenha, ao menos:
a) o seu número de série;
b) o nome do seu titular e, em se tratando de pessoa jurídica, o nome do responsável pelo seu uso, e a sua respectiva chave de verificação de assinatura;
c) a identificação e a assinatura eletrônica avançada do prestador de serviços de certificação credenciado que o emitiu;
d) a data de início e de fim de seu prazo de validade;
e) as restrições ao âmbito de sua utilização, se for o caso;
f) as restrições ao valor das transações nas quais pode ser utilizado, se for o caso;
g) outros elementos definidos nas normas complementares a esta Lei;

IX – prestador de serviços de certificação, a pessoa jurídica que emite certificados e presta outros serviços relacionados com assinaturas eletrônicas;
X – prestador de serviços de certificação credenciado, o prestador de serviço de certificação autorizado a emitir certificados no âmbito da ICP-Brasil;
XI – prestador de serviço de carimbo de tempo, a pessoa jurídica que atesta a data e a hora da assinatura, expedição ou recepção de um documento eletrônico e presta outros serviços relacionados com datação;
XII - prestador de serviço de carimbo de tempo credenciado, o prestador de serviço de carimbo de tempo autorizado a prestar o serviço de datação no âmbito da ICP-Brasil;
XIII - órgão de registro, órgão operacionalmente vinculado a um prestador de serviço de certificação, que processa as solicitações de emissão e de revogação de certificados qualificados, valida a identidade dos usuários, e desempenha outras atividades correlatas;
XIV - órgão de registro credenciado, o órgão de registro autorizado a desempenhar suas atividades no âmbito da ICP-Brasil;
XV – prestador de serviço de suporte, a pessoa natural ou jurídica que disponibiliza recursos humanos especializados e/ou infra-estrutura física e lógica a um prestador de serviço de certificação ou a um órgão de registro;
XVI – prestador de serviço de suporte credenciado, o prestador de serviço de suporte autorizado a funcionar no âmbito da ICP-Brasil;
XVII - componentes de aplicação de assinatura, os produtos físicos (hardware) e lógicos (software) que:
a) vinculem ao documento eletrônico processo de produção e verificação de assinaturas eletrônicas; ou
b) verifiquem assinaturas eletrônicas e confiram certificados, disponibilizando os resultados;
XVIII – componentes técnicos para serviços de certificação, os produtos físicos (hardware) e lógicos (software) que:
a) gerem chaves de assinatura, transferindo-as para um dispositivo seguro de criação de assinatura; ou
b) mantenham certificados disponíveis ao público para verificação por rede de computadores.

Parágrafo único. Equiparam-se a pessoa jurídica, para os fins do inciso IX, os que exerçam os serviços notariais e de registro por delegação do poder público, nos termos do art. 236 da Constituição Federal.

CAPÍTULO II - DAS ASSINATURAS E DOS DOCUMENTOS ELETRÔNICOS

Art. 3º A aposição de uma assinatura eletrônica deve referir-se inequivocamente a uma pessoa natural ou jurídica e ao documento eletrônico ao qual é aposta.

Art. 4º A assinatura eletrônica será reconhecida quando aposta durante o prazo de validade do certificado em que está baseada e respeitadas as restrições indicadas neste.
Parágrafo único. A assinatura eletrônica aposta após a revogação do certificado em que está baseada ou que não respeite as restrições indicadas neste equivale à ausência de assinatura.
Art. 5º As assinaturas eletrônicas avançadas têm o mesmo valor jurídico e probante das assinaturas manuscritas, na forma do art. 219 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil.

Art. 6º Não serão negados efeitos jurídicos ao documento eletrônico, desde que admitido como válido pelas partes ou aceito pela pessoa a quem seja oposto, pelo simples fato de sua assinatura eletrônica não ter sido gerada com base em certificado qualificado ou dispositivo seguro de criação de assinaturas.
Parágrafo Único – Nos casos em que importem transferência de domínio imobiliário ou envolvam interesse de incapazes, para oponibilidade dos efeitos jurídicos perante terceiros, o documento eletrônico deverá atender às exigências da legislação civil, processual e de registros públicos em vigor.

Art. 7º Os órgãos do Poder Judiciário poderão utilizar meio eletrônico para publicação de seus atos processuais.
Parágrafo único. A contagem dos prazos processuais terá início na data da publicação realizada na forma deste artigo.

CAPÍTULO III - DOS CERTIFICADOS DIGITAIS

Art. 8º O certificado qualificado será emitido a um titular, pessoa natural ou jurídica.
§ 1º Sendo titular uma pessoa jurídica, esta designará uma pessoa natural como responsável pelo uso do certificado.
§ 2º O titular ou o responsável pelo uso do certificado gerará o par de chaves criptográficas e responderá pela guarda e pelo uso exclusivo da chave de criação de assinatura.
§3º O titular de certificado ou o responsável pelo seu uso deve comunicar ao prestador de serviços de certificação ou ao órgão de registro a ele vinculado qualquer violação da confidencialidade de sua chave de criação de assinatura ou de sua mídia armazenadora, solicitando a revogação do correspondente certificado."
§4º Os dados constantes do certificado são públicos e disponíveis a qualquer interessado.

Art. 9º O certificado qualificado será revogado:
I – por solicitação do titular ou do responsável pelo uso;
II - caso seja comunicada a violação da confidencialidade da chave de criação de assinatura ou da sua mídia armazenadora;
III – caso constatada emissão imprópria ou defeituosa do mesmo;
IV – caso tenha sido emitido com base em dados falsos;
V – caso seja constatada a inexatidão ou desatualização de qualquer dos dados nele constante;
VI – por determinação judicial;
VII – em outros casos definidos pelo Comitê Gestor.
§ 1º A decisão de revogação do certificado qualificado com fundamento nos incisos III a VI será sempre motivada pelo prestador de serviço de certificação credenciado e comunicada ao titular e ao responsável pelo uso.
§ 2º Os certificados revogados na forma dos incisos e aqueles que perderam sua validade pelo término de seu prazo deverão ser publicados imediatamente na lista de certificados revogados pelo prestador de serviço de certificação que os emitiu.

Art. 10º As aplicações e os demais programas que admitirem o uso de certificado qualificado de um determinado tipo devem aceitar qualquer certificado qualificado de mesmo tipo ou com requisitos de segurança mais rigorosos.

Art. 11. Tratados, acordos ou atos internacionais poderão atribuir aos certificados emitidos no exterior os mesmos efeitos do certificado de que trata o inciso VIII, do art. 2°, observado o princípio da reciprocidade e obedecida a legislação brasileira, em matéria de registros públicos.
Parágrafo único. Tratados, acordos ou atos internacionais poderão atribuir aos certificados emitidos no exterior os mesmos efeitos do certificado de que trata o inciso VIII, do art. 2º, observado o princípio da reciprocidade.

TÍTULO II – DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

CAPÍTULO I - DAS DISPOSIÇÕES GERAIS

Art. 12. A certificação digital realizada no âmbito da ICP-Brasil se sujeitará aos preceitos desta Lei e ao que dispuser, ainda, o seu Comitê Gestor.

Art. 13. A ICP-Brasil tem como objetivo garantir a autenticidade, a integridade e validade jurídica das assinaturas em forma eletrônica, para a segurança das transações eletrônicas, aplicações de suporte e aplicações habilitadas que utilizem certificados qualificados.

Art. 14. A ICP-Brasil é composta por uma Autoridade Gestora de Políticas – Comitê Gestor, por uma Autoridade Certificadora Raiz – AC Raiz e, ainda, pelas seguintes entidades credenciadas:
I - prestadores de serviço de certificação;
II - órgãos de registro;
III - prestadores de serviço de suporte; e
IV - prestadores de serviço de carimbo de tempo.

CAPÍTULO II - DO COMITÊ GESTOR

Art. 15 Compete ao Comitê Gestor da ICP-Brasil:
I – coordenar o funcionamento da ICP-Brasil;
II – estabelecer a política, os critérios e as normas técnicas para o credenciamento dos prestadores de serviço de certificação, órgãos de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo de tempo, em todos os níveis da cadeia de certificação;
III – estabelecer a política de certificação e as regras operacionais da AC Raiz;
IV – homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço de suporte;
V – estabelecer diretrizes e normas técnicas para a formulação de políticas de certificado e regras operacionais dos prestadores de serviço de certificação, órgãos de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo de tempo credenciados na ICP-Brasil;
VI – identificar e avaliar as políticas de infra-estruturas de certificação externas, negociar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais e a legislação brasileira em matéria de registros públicos;
VII – dispor sobre os tipos de certificados no âmbito da ICP-Brasil; e
VIII – atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Art. 16 O Comitê Gestor da ICP-Brasil será integrado por:
I – sete representantes do Poder Executivo;
II – um representante do Senado Federal;
III – um representante da Câmara dos Deputados;
IV – cinco representantes do Poder Judiciário,sendo:
a) um representante do Supremo Tribunal Federal;
b) um representante do Superior Tribunal de Justiça;
c) um representante do Tribunal Superior do Trabalho;
d) um representante do Tribunal Superior Eleitoral;
e) um representante do Superior Tribunal Militar".
V – um representante do Ministério Público Federal; e
VI – dezesseis representantes da sociedade civil.
§1º A coordenação do comitê competirá ao Poder Executivo.
§2º Os representantes da sociedade civil serão designados, na forma do regulamento, para períodos de dois anos, permitida a recondução.
§3º A participação no comitê é de relevante interesse público e não será remunerada.
§4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

CAPÍTULO III - DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Art. 17. O Instituto Nacional de Tecnologia da Informação - ITI, autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz da ICPBrasil.

Art. 18. Ao ITI compete:

I - executar as políticas de certificação e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;
II - propor a revisão e a atualização das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;
III - credenciar e autorizar o funcionamento dos prestadores de serviço de certificação, órgãos de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo de tempo na ICP-Brasil;
IV - aprovar políticas de certificado, práticas de certificação e regras operacionais dos prestadores de serviço de certificação, órgãos de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo de tempo credenciados na ICP-Brasil;

V - gerenciar os certificados dos prestadores de serviço de certificação de nível imediatamente subseqüente ao seu, incluindo emissão, expedição, distribuição e revogação desses documentos eletrônicos;
VI - gerenciar a sua lista de certificados revogados;
VII - executar as atividades de fiscalização e de auditoria dos prestadores de serviço de certificação, órgãos de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo de tempo credenciados na ICP-Brasil, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor;
VIII - aplicar sanções e penalidades na forma da Lei;
IX - promover o relacionamento com instituições congêneres no País e no exterior;
X - celebrar e acompanhar a execução de convênios e acordos internacionais de cooperação, no campo das atividades de infra-estrutura de chaves públicas e áreas afins;
XI - estimular a participação de universidades, instituições de ensino e iniciativa privada em pesquisa e desenvolvimento, nas atividades de interesse da área da segurança da informação e da infra-estrutura de chaves públicas;
XII - desenvolver e disseminar soluções em software aberto e livre na Administração Pública Federal;
XIII – implementar soluções para a defesa da privacidade e segurança nos programas de inclusão digital;
XIV - executar outras atribuições que lhe forem cometidas pelo Comitê Gestor da ICP-Brasil.
§ 1º A AC Raiz não emite certificados para o usuário final.
§ 2º O Comitê Gestor poderá delegar atribuições à AC Raiz, salvo aquelas referentes à edição de atos de caráter normativo e aquelas que, pela sua própria natureza, só possam ser por ele implementadas.”

CAPÍTULO IV - DAS ENTIDADES CREDENCIADAS NA ICP-BRASIL

Art. 19. Aos prestadores de serviço de certificação, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados; manter registros de suas operações; bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes.
Parágrafo único. É vedado a qualquer prestador de serviço de certificação credenciado certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 20. Aos órgãos de registro, entidades credenciadas e vinculadas a um prestador de serviço de certificação, compete processar as solicitações de emissão de certificados, validar a identidade do titular e do responsável pelo uso do certificado, bem como desempenhar outras atividades correlatas.

Art. 21. Aos prestadores de serviço de suporte, entidades credenciadas e vinculadas a um prestador de serviço de certificação ou a um órgão de registro compete, dentre outras atividades correlatas, disponibilizar recursos humanos especializados e/ou infra-estrutura física e lógica.

Art. 22. Aos prestadores de serviço de carimbo de tempo, entidades credenciadas a prestar o serviço de datação no âmbito da ICP-Brasil compete atestar a data e a hora da assinatura, expedição ou recepção de um documento eletrônico.
§ 1º A hora a ser utilizada pelos prestadores de serviço de carimbo de tempo credenciados na ICP-Brasil será a oficial fornecida pela Observatório Nacional.
§ 2º Os sinais primários para sincronização de freqüência e tempo serão distribuídos pelo Observatório Nacional.

TÍTULO III - DA PRESTAÇÃO DE SERVIÇOS DE CERTIFICAÇÃO NO ÂMBITO DA ICP-BRASIL

CAPÍTULO I - DO CREDENCIAMENTO

Art. 23. A prestação de serviço de certificação fora do âmbito da ICP-Brasil não se sujeita à prévia autorização do Poder Público, sendo facultativa a solicitação de credenciamento.

Art. 24. O processo de credenciamento dos prestadores de serviço de certificação, órgãos de registro, prestadores de serviço de suporte e provedores de serviço de certificação de data e hora será disciplinado pelo Comitê Gestor, além das regras descritas nesta Lei.

Art. 25. O prestador de serviço de certificação poderá ser credenciado, mediante requerimento a ser encaminhado à AC Raiz, desde que:
I – comprove o cumprimento das diretrizes e normas técnicas, bem como das regras operacionais e práticas de certificação editadas pelo Comitê Gestor e pela AC Raiz da ICP-Brasil;
II – mantenha contrato de seguro em vigor, celebrado no Brasil, para cobertura da responsabilidade civil decorrente da atividade de certificação digital e de registro, em conformidade às normas complementares a esta Lei;
III – disponha de profissionais que comprovadamente tenham o conhecimento, a experiência e a qualificação necessários ao exercício da atividade;
IV - garanta que o par de chaves criptográficas seja gerado sempre pelo titular ou pelo responsável pelo uso do certificado, e que seja mantida a confidencialidade da chave de criação de assinatura;
V – demonstre possuir mecanismos e procedimentos adequados a impedir a falsificação ou deturpação de certificados;
VI – utilize sistema seguro de armazenamento de certificados, de modo que, pelo menos:
a) a autenticidade das informações possa ser verificada;
b) quaisquer alterações de caráter técnico suscetíveis de prejudicar esses requisitos de segurança sejam imediatamente detectáveis pelo operador;
VII – possua sistemas de proteção de dados adequados para impedir o uso indevido das informações e dos documentos fornecidos pelos titulares e pelos responsáveis pelo uso de certificados;
VIII – suas instalações operacionais e seus recursos de segurança física e lógica estejam localizados no território nacional;
IX - assegure que o órgão de registro operacionalmente vinculado ao mesmo realize a identificação e o cadastramento dos titulares e dos responsáveis pelo uso de certificados somente mediante a presença física desses, bem como mantenham os documentos por eles fornecidos pelo período de tempo disposto nas normas complementares a esta Lei;
X – implemente práticas eficazes de informação do usuário, inclusive sobre os efeitos jurídicos produzidos pelo certificado emitido e as medidas necessárias para proteção e segurança da chave de criação de assinatura;
XI – garanta o funcionamento de diretório rápido e seguro e de serviço de revogação de certificados seguro e imediato;
XII – assegure com precisão a possibilidade de verificação da data e hora de emissão ou revogação de cada certificado, utilizando a hora oficial fornecida pelo Observatório Nacional;
XIII – utilize componentes de aplicação de assinatura e componentes técnicos para serviços de certificação que atendam os requisitos definidos nos arts. 30 e 31 desta Lei;
XIV – adote sistemas e produtos seguros que estejam protegidos contra modificações e garantam a segurança técnica e criptográfica dos processos utilizados;
XV – armazene as chaves de verificação de assinaturas dos certificados por ele emitidos pelo prazo mínimo de 30 (trinta) anos, a contar da data da revogação ou da expiração dos mesmos, para verificação de assinaturas geradas durante seu período de validade;
XVI – demonstre qualificação econômico-financeira na forma das normas complementares a esta Lei; e
XVII – obrigue-se a transferir a outro prestador de serviço de certificação credenciado ou à AC Raiz todos os documentos e dados necessários à preservação dos certificados qualificados emitidos, em caso de encerramento de suas atividades.
Parágrafo único. A exigência prevista no inciso II não se aplica às entidades da administração pública federal direta, autárquica ou fundacional.”

Art. 26. O credenciamento do prestador de serviço de certificação implicará a emissão de seu certificado pela AC Raiz ou por prestador de serviço de certificação já credenciado na ICP-Brasil, na forma do parágrafo único do art. 18.

Art. 27. O ato de credenciamento do prestador de serviço de certificação pela ICP-Brasil indicará quais os tipos de certificados que este está autorizado a emitir.
§ 1º Caso o credenciamento limite a autorização a determinados tipos de certificados, o prestador de serviço de certificação poderá, a qualquer tempo, solicitar nova autorização à emissão de outros tipos de certificados.

§ 2º O certificado emitido por prestador de serviço de certificação credenciado, e em conformidade à autorização de que trata o caput, conterá a informação de que é um “certificado qualificado”, sendo vedado o emprego desta expressão para designar quaisquer outros certificados.

Art. 28. O disposto nos incisos I, II, III, VII, VIII e XVI do art. 24 aplica-se ao credenciamento dos prestadores de serviço de carimbo de tempo.
Parágrafo único. O seguro para cobertura da responsabilidade civil decorrente da atividade de datação deverá ser contratado em conformidade às normas complementares a esta Lei.

CAPÍTULO II - DOS COMPONENTES DE APLICAÇÃO E DOS COMPONENTES TÉCNICOS

Art. 29. A assinatura de documentos eletrônicos, decorrente de certificados qualificados, exige o uso de componentes de aplicação de assinatura que indiquem a produção de uma assinatura eletrônica avançada, e permita a identificação do documento a que a assinatura se refere.

Art. 30. Os componentes de aplicação de assinatura conterão, conforme dispuser o Comitê Gestor, mecanismos que demonstrem:
I – a que documento a assinatura se refere;
II – se o documento não foi modificado;
III – a que titular de certificado está vinculado o documento; e
IV – o conteúdo do certificado em que está baseada a assinatura.

Art. 31. Os componentes técnicos para serviços de certificação conterão, conforme dispuser o Comitê Gestor, mecanismos que:
I – assegurem que as chaves de criação de assinatura produzidas e transferidas a dispositivo seguro de criação de assinatura sejam únicas e sigilosas; e
II – protejam os certificados que estejam disponíveis para verificação e obtenção na rede de alterações, cópias ou obtenções (download) não autorizadas.

CAPÍTULO III - DOS DEVERES DAS PRESTADORAS DE SERVIÇOS DE CERTIFICAÇÃO

Art. 32. O prestador de serviço de certificação credenciado deverá, no momento da solicitação de emissão de um certificado qualificado, informar o solicitante, prévia e adequadamente sobre:
I – os efeitos jurídicos das assinaturas eletrônicas avançadas;
II – a forma de geração do par de chaves criptográficas;
III – as medidas necessárias para a proteção e segurança da chave de criação de assinatura;
IV – as medidas necessárias para a verificação de assinaturas eletrônicas de maneira confiável; e
V – os casos e as formas de revogação do certificado.
Parágrafo único. Os contratos de prestação de serviço de certificação digital serão redigidos em termos claros e com caracteres legíveis, de modo a facilitar a compreensão de suas cláusulas.

Art. 33. O prestador de serviço de certificação credenciado deverá informar os titulares de certificados qualificados por ele emitidos do encerramento de suas atividades, para que estes possam:
I – solicitar a revogação de seu certificado; ou
II – autorizar a transferência de sua documentação a outro prestador de serviço de certificação credenciado para preservação do certificado.
Parágrafo único. A informação de que trata o caput será prestada após o disposto no § 1º do art. 41.

Art. 34. O prestador de serviço de certificação credenciado é obrigado a manter confidencialidade sobre todas as informações obtidas do titular que não constem do certificado qualificado.
§ 1º Os dados pessoais não serão usados para outra finalidade que não a de certificação, salvo se consentido expressamente pelo requerente, por cláusula em destaque, que não vincule a prestação do serviço de certificação.
§ 2º A quebra da confidencialidade das informações de que trata o caput deste artigo, quando determinada pelo Poder Judiciário, respeitará os mesmos procedimentos previstos em lei para a quebra do sigilo bancário.

CAPÍTULO IV - DA RESPONSABILIDADE PELA PRESTAÇÃO DO SERVIÇO DE CERTIFICAÇÃO

Art. 35. As entidades integrantes da ICP-Brasil, inclusive a AC Raiz, respondem diretamente pelos danos a que derem causa.

Art. 36. Os prestadores de serviço de certificação respondem solidariamente pelos danos a que derem causa os prestadores de serviço de certificação por eles diretamente certificados, em caso de desatendimento dos requisitos constantes do artigo 25, bem como os órgãos de registro e os prestadores de serviço de suporte a eles vinculados.

Art. 37. São nulos de pleno direito os itens das políticas de certificado e das práticas de certificação, bem como as cláusulas dos contratos de prestação de serviço de certificação, que impossibilitem, exonerem ou atenuem a responsabilidade do prestador de serviço de certificação por vícios de qualquer natureza dos serviços por eles prestados.
Parágrafo único. Em situações justificáveis, poderá ocorrer limitação da indenização quando o titular do certificado for pessoa jurídica.

CAPÍTULO V - DA MANUTENÇÃO DO CREDENCIAMENTO E DO ENCERRAMENTO DAS ATIVIDADES

Art. 38. Para fins de manutenção do credenciamento na ICP-Brasil, os prestadores de serviço de certificação devem observar o disposto nos incisos I a XVII do art. 24 e o seu descumprimento ensejará a aplicação das penalidades dispostas no art. 42.

Art. 39. O disposto no art. 27 deve ser observado pelos prestadores de serviço de carimbo de tempo para fins de manutenção do seu credenciamento na ICP-Brasil.

Art. 40. O prestador de serviço de certificação encerrará suas atividades no âmbito da ICP-Brasil por determinação da AC Raiz, no caso de descredenciamento, ou ainda por ato voluntário.

Art. 41. O encerramento das atividades de prestador de serviço de certificação credenciado pela ICP-Brasil implicará a transferência a outro prestador de serviço de certificação credenciado de todos documentos e dados necessários à preservação dos certificados qualificados emitidos.
§1º Havendo interesse de mais de um prestador de serviço de certificação credenciado, a transferência será àquele indicado pela entidade que está encerrando suas atividades, após aprovação da AC Raiz.
§ 2º Caso não haja interesse de nenhum prestador de serviços de certificação credenciado, a transferência de que trata o caput será feita à AC Raiz.

CAPÍTULO VI - DA INFRAÇÃO E DAS PENALIDADES

Art. 42. A AC Raiz poderá tomar as medidas necessárias para prevenir ou coibir a prática de atos contrários a esta Lei ou às suas normas complementares, praticados pelos prestadores de serviço de certificação, órgãos de registro, prestadores de serviço de suporte ou prestadores de serviço de carimbo de tempo credenciados na ICP-Brasil.

Art. 43. A infração por prestador de serviço de certificação credenciado a qualquer dispositivo desta Lei ou das normas complementares editadas pelo Comitê Gestor, assim como as determinações exaradas pela AC Raiz da ICP-Brasil, implicará a aplicação das seguintes penalidades, conforme a gravidade da infração e na forma da Lei:
I – advertência por escrito;
II – multa simples ou diária de R$ 100,00 (cem reais) a R$ 1.000.000,00 (um milhão de reais);
III – proibição de credenciamento de novas políticas de certificado;
IV – suspensão da emissão de novos certificados; e
V – descredenciamento.
§ 1º As penalidades poderão ser aplicadas isoladas ou cumulativamente.
§ 2º O descumprimento da penalidade disposta no inciso IV não impede a imposição de outra mais grave.
§ 3º A penalidade prevista no inciso V será aplicada, sem prejuízo de outras sanções cabíveis, quando:

I – o credenciamento for obtido por meio de declarações falsas ou outros meios ilícitos;
II - no exercício de atividade de prestação de serviço de certificação estiverem sendo praticados atos em desconformidade com esta lei ou com normas complementares editadas pelo Comitê Gestor.
§ 4º Da decisão de descredenciamento caberá pedido de reconsideração e recurso com efeito suspensivo, na forma das normas complementares a esta lei.

Art. 44. O disposto neste Capítulo aplica-se, no que couber, aos órgãos de registro, prestadores de serviço de suporte e prestadores de serviço de carimbo de tempo credenciados na ICP-Brasil.

TÍTULO IV - DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 45. Aplica-se, no que couber, à prestação de serviços de certificação e de datação, a legislação de defesa do consumidor e as normas processuais sobre a validade e prova documental.
Art. 46. Na administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, somente será admitido o uso de certificados qualificados.
Art. 47. O Poder Executivo disporá sobre o uso de certificados qualificados na emissão de passaportes, de documentos de identidade, de carteiras nacional de habilitação, de certificados de registros de veículos, bem como em outras aplicações.
Parágrafo único. Os documentos em papel copiados em meio eletrônico, cujo original tenha sido conferido, farão prova plena quando o tabelião atestar a conformidade com o original apondo sua assinatura digital.

Art. 48. As referências normativas a Autoridades Certificadoras – AC passam a ser entendidas como prestadores de serviços de certificação, exceto no caso da AC Raiz da ICP-Brasil; e as referências a Autoridades de Registro – AR passam a ser entendidas como órgãos de registro.

Art. 49. A constituição ou declaração de direitos e obrigações instrumentada em documento eletrônico deverá, nos casos que importem em transferência de domínio imobiliário ou envolvam interesse de incapazes, para ter validade perante terceiros, sujeitar-se às prescrições da legislação civil, processual e de registros públicos em vigor.

Art. 50. As entidades da Administração Pública Federal direta, autárquica e fundacional, credenciadas pela ICP-Brasil para prestar serviço de certificação, terão prazo de um ano, contado da publicação desta lei, para contratar o seguro a que se refere o inciso II do art. 24.

Art. 51. Fica revogada a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, sendo convalidados os atos praticados nela fundamentados.

Art. 52. Esta Lei entra em vigor na data de sua publicação.

DECRETO Nº 4.522 DE 17 DE DEZEMBRO DE 2002
Autor: Poder Executivo

Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências. O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso VI, alínea "a", da Constituição,

DECRETA:

Art. 1º. Ficam organizadas sob a forma de sistema, com a designação de Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, as atividades de elaboração, redação, alteração, controle, tramitação, administração e gerência das propostas de atos normativos a serem encaminhadas ao Presidente da República pelos Ministérios e órgãos integrantes da estrutura da Presidência da República.

Art. 2º. O SIDOF tem a seguinte estrutura:

I - órgão central - Casa Civil da Presidência da República, responsável pela formulação de diretrizes, orientação, planejamento, coordenação, supervisão e controle dos assuntos a ele relativos;
II - órgãos setoriais - unidades incumbidas especificamente de atividades concernentes ao Sistema nos Ministérios e órgãos integrantes da Presidência da República;
III - órgãos seccionais - unidades incumbidas da execução das atividades do SIDOF, nas autarquias e fundações públicas.

Art. 3º. Participam do SIDOF:

I - o Presidente da República;
II - os Ministros de Estado e os dirigentes máximos de órgãos integrantes da estrutura da Presidência da República, responsáveis pela proposição de documentos oficiais ao Presidente da República;
III - os titulares dos órgãos de assistência jurídica dos ministérios e da Presidência da República;
IV - o Administrador-Geral do SIDOF, designado pelo Subchefe para Assuntos Jurídicos da Casa Civil da Presidência da República, responsável pela formulação de diretrizes, orientação, planejamento, coordenação, supervisão e controle dos assuntos relativos ao Sistema;
V - o Administrador de Usuários e os responsáveis ou prepostos setoriais e seccionais incumbidos das atividades concernentes ao SIDOF, nos Ministérios e órgãos supervisionados, ou integrantes da Presidência da República;
VI - o órgão responsável pela infra-estrutura de tecnologia da informação, a cargo da Diretoria de Tecnologia da Informação da Secretaria de Administração da Casa Civil da Presidência da República, incumbido da implementação e atualização do SIDOF, abrangendo software básico e aplicações, bem como pela permanente coordenação das aplicações da tecnologia utilizada.
VII - a Coordenação-Geral de Certificação da Secretaria de Administração da Casa Civil como Autoridade Certificadora da Presidência da República; e
VIII - o órgão responsável pela infra-estrutura de equipamentos, manutenção e suporte técnico aos usuários do SIDOF, nos órgãos setoriais e seccionais a cargo das respectivas Coordenações de Modernização e Informática, ou equivalentes.

Art. 4º. Incumbe ao órgão central do SIDOF:

I - quanto à administração:
a) gerenciar o cadastramento de órgãos, Ministérios e Administradores de Usuários, atribuindo perfil de acesso para os responsáveis ou prepostos setoriais e seccionais;
b) bloquear ou modificar o acesso dos responsáveis ou prepostos setoriais e seccionais;
c) excluir, incluir ou modificar fluxos de documentos;
d) intervir no fluxo ou trâmite natural do documento, direcionando-o para a etapa que se fizer necessária;
e) acessar o histórico do Sistema e visualizar as ações realizadas;
f) manter relacionamento direto com os responsáveis ou prepostos do Sistema nos órgãos setoriais e seccionais, expedindo-lhes instruções;

g) expedir normas para disciplinar a utilização, padronização, envio e recepção de mensagens necessárias ao fiel funcionamento do Sistema;
h) supervisionar e coordenar a execução das normas de que tratam as alíneas "a" a "g"; e
i) executar outras atividades quando determinadas pelo Secretário-Executivo da Casa Civil.
II - quanto à instituição e manutenção do Sistema, por intermédio da Diretoria de Tecnologia da Informação da Secretaria de Administração da Casa Civil da Presidência da República:
a) a elaboração ou a contratação de serviços de terceiros para sua execução;
b) a disponibilização de informações técnicas aos órgãos setoriais e seccionais necessárias ao seu regular funcionamento;
c) prover os meios para o armazenamento e guarda das informações em banco de dados centralizado com sigilo, integridade e disponibilidade;
d) garantir restrição de acesso dos participantes do Sistema às funcionalidades e às informações efetivamente necessárias para a execução da atividade específica;
e) manter a operação da aplicação, garantindo os requisitos de segurança, disponibilidade e acessibilidade;
f) supervisionar e coordenar a execução das normas de que tratam as alíneas "a" a "e".
III - quanto à certificação digital dos participantes, sob a responsabilidade da Autoridade Certificadora da Presidência da República:
a) identificar e cadastrar os participantes do Sistema na presença destes;
b) emitir, expedir, distribuir, revogar e gerenciar os certificados digitais; e
c) assegurar à assinatura eletrônica, irretratabilidade, integridade e autenticidade pessoal.

Art. 5º. No âmbito dos órgãos setoriais e seccionais do SIDOF, incumbe:

I - aos Ministros de Estado apor as assinaturas digitais requeridas para o trâmite do respectivo documento oficial e autorizar o seu encaminhamento;
II - aos titulares de órgãos de assessoramento jurídico:
a) formular pareceres jurídicos e encaminhá-los ao preposto, para apreciação do Ministro de Estado; ou
b) apor a assinatura digital requerida no parecer para o trâmite do documento oficial, quando encaminhado pelo preposto;
III - ao Administrador de Usuários:
a) gerenciar as atividades do Sistema no âmbito de sua unidade administrativa;
b) propor ao Administrador-Geral a inclusão ou exclusão de participantes do Sistema; e
c) manter relacionamento direto com os responsáveis ou prepostos do Sistema nos órgãos seccionais, expedindo-lhes instruções.
IV - aos prepostos:
a) dar início ao trâmite do documento, providenciando a inclusão no Sistema dos textos dos atos normativos a serem encaminhados ao Presidente da República;
b) assessorar o Ministro de Estado e demais autoridades do respectivo Ministério quanto ao encaminhamento e à aposição de suas assinaturas digitais para o trâmite oficial do documento; e
c) tomar as providências necessárias à execução eficaz do trâmite do documento no âmbito de seu órgão ou entidade.

§ 1º Compete às Coordenações de Modernização e Informática dos Ministérios, ou equivalentes nos órgãos seccionais, o provimento de recursos técnicos e de suporte em informática aos participantes do SIDOF, em seus respectivos órgãos, necessários ao pleno funcionamento do Sistema.

§ 2º Os órgãos setoriais e seccionais do SIDOF prestarão ao órgão central todas as informações e o apoio necessário ao planejamento, coordenação, acompanhamento, fiscalização e controle das atividades previstas neste Decreto.
§ 3º Os responsáveis ou prepostos setoriais do SIDOF vinculam-se ao Administrador-Geral para os efeitos do disposto neste Decreto, sem prejuízo da subordinação administrativa decorrente de sua posição na estrutura do Ministério e órgãos da estrutura da Presidência da República.

Art. 6º. Incumbe ao Administrador-Geral do SIDOF:

I - gerenciar o cadastramento dos usuários do Sistema;

II - manter relacionamento de apoio e orientação operacional com todas as áreas e participantes do Sistema;
III - expedir normas para disciplinar a utilização, normatização, envio e recepção de mensagens; e
IV - praticar as atividades administrativas de que trata o inciso I do art. 4º.

Art. 7º. Os Secretários-Executivos dos Ministérios indicarão, ao Administrador-Geral do SIDOF, o Administrador de Usuários, em seu âmbito de atuação, responsável por registrar o cadastramento e exclusões de usuários, bem assim as ausências e afastamentos legais e regulamentares do titular da Pasta, após autorizados pelo Presidente da República.

Art. 8º. O SIDOF será implantado em fases, mediante ato do Chefe da Casa Civil da Presidência da República, abrangendo inicialmente as atividades entre o órgão central e os órgãos setoriais.

Parágrafo único. Realizar-se-ão, sob a forma de auditoria, a cargo da Subchefia para Assuntos Jurídicos da Casa Civil da Presidência da República, o controle, a fiscalização e a orientação específica das atividades do SIDOF.

Art. 9º. O Chefe da Casa Civil da Presidência da República poderá baixar normas complementares para a execução do disposto neste Decreto.

Art. 10. Este Decreto entra em vigor na data de sua publicação.

PROJETO DE LEI DO SENADO Nº 229 DE 22 DE JUNHO DE 2005

Autor: Sen. Pedro Simon

Dispõe sobre a autenticidade e o valor jurídico e probatório de documentos produzidos, emitidos ou recebidos por órgãos públicos federais, estaduais e municipais, por meio eletrônico.

O Congresso Nacional decreta:

Art. 1º Os documentos produzidos, emitidos ou recebidos por órgãos públicos federais, estaduais ou municipais, bem como pelas empresas públicas, por meio eletrônico ou similar, têm o mesmo valor jurídico e probatório, para todos os fins de direito, que os produzidos em papel ou em outro meio físico reconhecido legalmente, desde que assegurada a sua autenticidade e integridade.

Parágrafo único. A autenticidade e integridade serão garantidas pela execução de procedimentos lógicos, regras e práticas operacionais estabelecidas pelo Poder Público, na forma que dispõe a Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

Art. 2º A cópia, traslado ou transposição de documento em papel ou em outro meio físico para o meio eletrônico somente terá validade se observados os requisitos estabelecidos nesta Lei e em seu regulamento.

Art. 3º A reprodução em papel ou em outro meio físico de documento eletrônico somente terá validade jurídica se autenticada na forma do regulamento.

Art. 4º O documento eletrônico a que se refere esta Lei deverá ser acessível, legível e interpretável segundo os padrões correntes em tecnologia da informação.

Art. 5º Fica autorizado o arquivamento por meio magnético, óptico, eletrônico ou similar, de documentos públicos ou particulares.

Art. 6º Atendido o disposto nesta Lei, os documentos arquivados na forma do artigo anterior, assim como suas certidões, traslados e cópias obtidas diretamente dos respectivos arquivos, em meio magnético, óptico, eletrônico ou similar, produzirão, para todos os fins de direito, os mesmos efeitos legais dos documentos originais.

Art. 7º O arquivamento deverá garantir a integridade e autenticidade dos documentos, assegurando, ainda, que:

I - sejam acessíveis e que os respectivos dados e informações possam ser lidos e interpretados no contexto em que devam ser utilizados;
II - permaneçam disponíveis para consultas posteriores;
III - sejam preservados no formato em que foram originalmente produzidos.

Art. 8º O sistema de arquivamento na forma autorizada por esta Lei deverá ainda:
I - manter equipamentos de computação necessários para a recuperação e a exibição dos dados arquivados, durante o prazo em que as respectivas informações permanecerem úteis;
II - dispor de métodos e processos racionais de busca e trilhas de auditoria;
III - conter dispositivos de segurança contra acidentes e emergências, capazes de evitar a destruição ou qualquer dano que impossibilite o acesso aos dados arquivados ou em processo de arquivamento.

Art. 9º Os documentos em papel ou em outro meio físico e que tenham sido arquivados em meio magnético, óptico, eletrônico ou similar poderão, a critério da autoridade competente, ser eliminados por incineração, destruição mecânica ou outro processo adequado para este fim.

§ 1º A eliminação a que se refere o caput far-se-á mediante lavratura de termo circunstanciado, por autoridade competente.

§ 2º Os documentos de valor histórico não serão eliminados, e poderão ser arquivados em local diverso da repartição que os detenha, para sua melhor conservação.

Art. 10. Esta Lei entra em vigor na data de sua publicação.

PROJETO DE LEI DA CÂMARA Nº 6.693 DE 7 DE MARÇO DE 2006

Autor: Dep. Sandra Rosado

Altera o art. 375 da lei no 5.869, de 11 de janeiro de 1973 - Código de Processo Civil.

O Congresso Nacional decreta:

Art. 1º Esta lei altera a redação do o art. 375 da lei no 5.869, de 11 de janeiro de 1973 - Código de Processo Civil.

Art. 2º O art. 375 da lei no 5.869, de 11 de janeiro de 1973 - Código de Processo Civil passa a vigorar com a seguinte redação :

"Art. 375. O telegrama, o radiograma ou o e-mail presume-se conforme com o original, provando a data de sua expedição e do recebimento pelo destinatário."

Art. 3º Esta lei entra em vigor na data de sua publicação.

MENSAGEM DA PRESIDÊNCIA Nº 268 DE 24 DE ABRIL DE 2006

Senhores Membros do Congresso Nacional

Solicito a Vossas Excelências, de conformidade com a Exposição de Motivos da Senhora Ministra de Estado Chefe da Casa Civil, a retirada de tramitação do Projeto de Lei n° 2.281, de 2003, que “Institui a Taxa de Credenciamento – TCD, a Taxa de Fiscalização e de Manutenção de Credenciamento – TFM, as multas que especifica, e dá outras providências”, enviado à Câmara dos Deputados com a Mensagem n° 510, de 2003.

Excelentíssimo Senhor Presidente da República,

Submeto à elevada consideração de Vossa Excelência solicitação de retirada de tramitação do Projeto de Lei n° 2.281, de 2003, que “Institui a Taxa de Credenciamento – TCD, a Taxa de Fiscalização e de Manutenção de Credenciamento – TFM, as multas que especifica, e dá outras providências”.

2. O ITI é uma Autarquia Federal designada para exercer a função de Autoridade Certificadora Raiz da ICP-Brasil, conforme Medida Provisória n° 2.200-2, de 24 de agosto de 2001, e, como autarquia, deveria possuir autonomia financeira, conforme preconiza o Decreto-Lei n° 200, de 1967. Desde sua criação, porém, subsiste com verbas repassadas.

3. O Projeto de Lei n° 2.281, de 2003, foi elaborado com a finalidade de criar política arrecadatória própria para sustentação do Instituto, baseada na cobrança de taxas sobre as atividades de credenciamento, manutenção de credenciamento e fiscalização das entidades vinculadas à ICP-Brasil, atividades essas que são de responsabilidade do ITI.

4. Ocorre que a política arrecadatória proposta, considerados os valores das taxas estipuladas no Projeto de Lei n° 2.281, de 2003, e a quantidade de entidades atualmente credenciadas, não permitiria, hoje, sustentar as atividades do Instituto.

5. Por fim, observamos que os termos em que a matéria é tratada no Projeto de Lei n° 2.281, de 2003, já não mais se coadunam com aqueles utilizados no Projeto de Lei n° 7.316, de 2002, que visa substituir a Medida Provisória n° 2.200-2, de 2001, disciplinando o uso de assinaturas eletrônicas e prestação de serviços de certificação digital no Brasil

6. Diante dessas considerações, submeto à apreciação de Vossa Excelência proposta no sentido de que o referido Projeto de Lei seja retirado de tramitação no Congresso Nacional, para que esta Casa Civil possa reavaliar a matéria.

ANEXO II – TABELA COMPARATIVA DA LEGISLAÇÃO ESTRANGEIRA

País	Portugal	República Tcheca	Irlanda	Peru
Instrumento legal	Decreto-Lei nº 290-D/99	Ato nº 227, de 29/6/2000 (The Electronic Sig. Act)	Electronic Com-merce Act, 2000	Ley nº 27269
A legislação inclui definições dos principais termos usados	SIM	SIM	SIM	NÃO (Remete para o regulamento)
Trata da validade do documento eletrônico	SIM	SIM (mensagem eletrônica)	SIM	NÂO
Trata da assinatura eletrônica	SIM	SIM	SIM	SIM
É neutra tecnologicamente	NÃO (criptografia assimétrica)	SIM	SIM	NÃO (criptografia assimétrica)
Trata da certificação	SIM	SIM	SIM	SIM
Admite o credenci-amento da entidade certificadora	SIM (voluntário)	SIM (voluntário) (Administração pública só aceita documento eletrônico certificado por entidade credenciada	SIM (voluntário)	SIM (voluntário) (compulsório o registro)
Trata de certificadoras de outro país	SIM	SIM	NÃO	SIM
Trata da proteção à privacidade	SIM (somente de informações prestadas às entidades certificadoras)	NÃO	NÃO	SIM (somente de informações prestadas às entidades certificadoras)
Trata da proteção ao consumidor	NÃO	SIM (remete à legislação específica)	SIM	NÃO
Trata dos deveres e responsabilidades dos intermediários (provedores)	NÃO	NÃO	NÃO	NÃO
Inclui disposições tributárias	NÃO	NÃO	NÃO	NÃO

Tabela 11.1 – Análise comparativa da legislação adotada em outros países e por organismos internacionais. Fonte: Semeghini, J. Acessado em 07/07/2006 em http://www.cbeji.com.br.

País	Colômbia	Espanha	Alemanha	Hong-Kong
Instrumento legal	Ley 527 de 1999	Real Decreto-ley 14/1999	Law Governing Framework Conditions for Electronic Signatures	Electronic Transactions Ordinance
A legislação inclui definições dos principais termos usados	SIM	SIM	SIM	SIM
Trata da validade do documento eletrônico	SIM (mensagem eletrônica)	NÃO	NÃO	SIM
Trata da assinatura eletrônica	SIM	SIM	SIM	SIM
É neutra tecnologicamente	NÃO (criptografia assimétrica)	SIM	NÃO (criptografia assimétrica)	NÃO (criptografia assimétrica)
Trata da certificação	SIM	SIM	SIM	SIM
Admite o credenciamento da entidade certificadora	SIM (compulsória)	SIM (voluntária)	SIM (voluntária)	SIM (voluntária)
Trata de certificadoras de outro país	SIM	SIM	SIM	SIM
Trata da proteção à privacidade	NÃO	NÃO	SIM (somente de informações prestadas às entidades certificadoras)	SIM (somente de informações prestadas às entidades certificadoras)
Trata da proteção ao consumidor	NÃO	NÃO	NÃO	NÃO
Trata dos deveres e responsabilidades dos intermediários (provedores)	NÃO	NÃO	NÃO	NÃO
Inclui disposições tributárias	NÃO	NÃO	NÃO	NÃO

Tabela 12.1 (continuação) – Análise comparativa da legislação adotada em outros países e por organismos internacionais. Fonte: Semeghini, J. Acessado em 07/07/2006 em http://www.cbeji.com.br.

País	Cingapura	Estados Unidos	Com. Européia	UNCITRAL
Instrumento legal	Electronic Transactions Act	Electronic Signatures in Global and National Commmerce Act	Diretiva 99/93-CE	Lei Modelo
A legislação inclui definições dos principais termos usados	SIM	NÃO	SIM	SIM
Trata da validade do documento eletrônico	SIM	SIM (mensagem eletrônica)	SIM	SIM (mensagem eletrônica)
Trata da assinatura eletrônica	SIM	SIM	SIM	SIM
É neutra tecnologicamente	NÃO (criptografia assimétrica)	SIM	SIM	SIM
Trata da certificação	SIM	NÃO	SIM	NÃO
Admite o credenciamento da entidade certificadora	SIM (voluntário)	NÃO	SIM (voluntário)	NÃO
Trata de certificadoras de outro país	SIM	NÃO	SIM	NÃO
Trata da proteção à privacidade	NÃO	NÃO	Remete a outra diretiva (95/46 – CE)	NÃO
Trata da proteção ao consumidor	NÃO	SIM (preserva direitos de outras legislações)	NÃO	NÃO
Trata dos deveres e responsabilidades dos intermediários (provedores)	SIM	NÂO	NÃO	NÃO
Inclui disposições tributárias	NÃO	NÃO	NÃO	NÃO

Tabela 12.1 (continuação) – Análise comparativa da legislação adotada em outros países e por organismos internacionais. Fonte: Semeghini, J. Acessado em 07/07/2006 em http://www.cbeji.com.br.